LIBERTÉS PUBLIQUES ET ÉTHIQUE

JUIN 2020

RECONNAISSANCE FACIALE : PORTER LES VALEURS DE L'EUROPE

RENAISSANCE numerique

TABLE DES MATIÈRES

CE QU'IL FAUT RETENIR ____ 5

INTRODUCTION - LES GARANTIES FONDAMENTALES D'UNE SOCIÉTÉ NUMÉRIQUE ____ 9

PARTIE 1 - LA MATURITÉ TECHNIQUE DES TECHNOLOGIES DE RECONNAISSANCE FACIALE OUVRE LA VOIE AU DÉPLOIEMENT DE LEURS USAGES ____ 15

Une maturité qui s'inscrit dans la dynamique des technologies d'intelligence artificielle ____ **16**

Le champ de la reconnaissance faciale représente une diversité d'usages ____ **20**

Des usages variés qui comportent différents niveaux de risques ____ 20

Le chevauchement avec d'autres technologies soulève également des interrogations ____ 27

Des technologies qui ne sont pas infaillibles ____ **28**

Les lacunes inhérentes des technologies de reconnaissance faciale ____ 28

Une course technologique perpétuelle pour corriger leurs effets négatifs ____ 35

Les lacunes humaines face à une technologie probabiliste ____ 37

PARTIE 2 - UN CADRE JURIDIQUE À L'APPLICATION DISPARATE ET PEU EFFICIENTE ____ 40

Les technologies de reconnaissance faciale : des dispositifs relativement bien encadrés juridiquement ____ **41**

Les droits fondamentaux applicables aux technologies de reconnaissance faciale ____ 42

Les réglementations nationales et régionales complètent le cadre esquissé par les droits fondamentaux ____ 51

Un cadre juridique qui pâtit de profondes faiblesses dans son application ____ **69**

Une application fluctuante parmi les États membres ____ 69

Des difficultés d'application qui entraînent un manque d'efficience ____ 71

PARTIE 3 - VERS UN SYSTÈME DE STANDARDISATION EUROPÉEN GARANT DES DROITS ET LIBERTÉS FONDAMENTAUX ____ 77

La prédominance du NIST dans le marché international de la standardisation ____ **79**

Les fondements de cette prédominance : une compétence reconnue à l'international et l'absence d'équivalent européen ____ 79

La nécessaire remise en cause de cette prédominance ____ 83

Faire des standards européens le levier de la protection des citoyens 84

Prendre en compte à la fois les aspects techniques et juridiques 86

Garantir l'adoption des standards européens en imposant leur respect dans les marchés publics 89

Une gouvernance européenne dédiée à la standardisation des technologies de reconnaissance faciale 91

Réunir les expertises au sein d'une instance multi-parties prenantes 91

Placer l'auditabilité au cœur du système de standardisation 95

CONCLUSION - L'OPPORTUNITÉ POUR L'UE DE REMETTRE L'HUMAIN AU CŒUR DU SYSTÈME 98

CE QU'IL FAUT RETENIR

Les technologies de reconnaissance faciale : des outils probabilistes qui traitent de données sensibles

- Les technologies de reconnaissance faciale reposent sur des méthodes d'intelligence artificielle qui appliquent des techniques dites d'apprentissage profond (*deep learning*) au domaine de la vision par ordinateur, permettant de reconnaître des visages sur des images (vidéo ou fixes) en s'appuyant sur des données biométriques. Elles diffèrent donc des technologies de reconnaissance comportementale ou émotionnelle, qui elles reposent par exemple sur l'analyse de la coordination des mains, des tremblements, du mouvement des yeux ou encore des muscles du visage.

- Le traitement des données biométriques est, en principe, interdit au sein de l'Union européenne (UE). Par leur recours à des données biométriques, les technologies de reconnaissance faciale sont donc hautement sensibles. Le recours à ces technologies doit être exceptionnel, et une alternative à ces dernières doit toujours être privilégiée.

- Les technologies de reconnaissance faciale regroupent des technologies extrêmement diverses. Tous les usages (public ou privé, consenti ou à l'insu des individus, en temps réel ou différé, etc.), ne comportent pas la même sensibilité et les mêmes facteurs de risque.

- Les technologies de reconnaissance faciale ne sont pas infaillibles. Leurs systèmes peuvent être sujets à des failles de sécurité importantes et certaines technologies peuvent induire des

biais pouvant provoquer des discriminations racistes, sexistes ou âgistes.

- Au-delà de ces lacunes d'ordre technique, certaines failles peuvent également résulter de l'intervention humaine dans l'interprétation des résultats de ces technologies qui sont probabilistes. Il est primordial que les utilisateurs de ces technologies soient formés à leur usage.

- Toute décision prise dans laquelle une technologie de reconnaissance faciale est impliquée est le résultat d'une chaîne d'événements. Dès lors, il est indispensable d'assurer l'explicabilité des décisions à chaque niveau de la chaîne, jusqu'à la décision humaine.

Le cadre juridique qui entoure les technologies de reconnaissance faciale est relativement complet en Europe, mais son application est disparate et peu efficiente

- Au sein de l'UE, les technologies de reconnaissance faciale sont relativement bien encadrées juridiquement, que ce soit par les droits fondamentaux, ou par divers textes européens (RGPD, Directive Police-Justice) et nationaux (Loi Informatique et Libertés par exemple pour la France) qui viennent les compléter.

- Ce cadre juridique pâtit toutefois de faiblesses dans son application, qui le rendent peu efficient.

- D'une part, la réglementation européenne est appliquée de manière fluctuante d'un État membre à l'autre, notamment dans le domaine de la recherche fondamentale. Les autorités de régulation nationales possèdent en outre des ressources humaines et financières disparates et insuffisantes pour bien le mettre en œuvre.

- D'autre part, ce cadre souffre de difficultés dans l'application des droits fondamentaux. Il est complexe d'assurer la conformité des technologies de reconnaissance faciale avec nos droits fondamentaux en l'absence de contrôle *a priori*. Quant aux analyses réalisées *ex post* par les juges, ces dernières demandent d'une part que le juge soit saisi, et d'autre part un investissement considérable de la part du requérant, notamment en termes de temps et de compétences.

Face à la prédominance américaine et pour garantir les droits et libertés fondamentaux des citoyens, l'Union européenne doit se doter d'un système robuste de standardisation européen des technologies de reconnaissance faciale

- Le National Institute for Standards and Technology (NIST) américain domine actuellement le marché international de la standardisation des technologies de reconnaissance faciale. Les critères d'évaluation établis par le NIST sont largement utilisés dans le monde, y compris au sein des appels d'offres européens. Ces standards font toutefois référence à des critères exclusivement techniques.

- Pour asseoir sa souveraineté numérique et protéger les droits et libertés fondamentaux de ses citoyens, l'UE doit définir ses propres standards et y intégrer des dimensions juridiques. Lorsqu'il s'agit de technologies de reconnaissance faciale, la fiabilité d'un système ne saurait en effet s'arrêter à ses seules performances techniques.

- Les technologies de reconnaissance faciale étant évolutives, leur conformité aux standards européens doit être régulièrement évaluée, ainsi que les standards eux-mêmes.

- L'adoption de ces standards doit passer par leur imposition dans le cadre des marchés publics européens, nationaux et locaux, expérimentations incluses. Cette obligation doit garantir leur adoption à grande échelle par un effet performatif.

- Au-delà de leur adoption, l'imposition de ces standards dans le

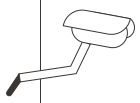
cadre des marchés publics doit permettre un encadrement effectif de la surveillance publique.

- Pour porter ses standards, l'UE doit s'appuyer sur une instance de gouvernance multi-parties prenantes, réunissant les expertises en matière de standardisation, de droits fondamentaux, dont la protection des données à caractère personnel, et plus globalement de défense des droits.

- La mise en œuvre du système de standardisation européen nécessite également des investissements (financiers et en ressources humaines) de la part des États membres, afin de garantir la montée en puissance des autorités de contrôle européennes.

INTRODUCTION
LES GARANTIES FONDAMENTALES D'UNE SOCIÉTÉ NUMÉRIQUE

Dans son livre blanc sur l'intelligence artificielle publié en février dernier, la Commission européenne annonce sa volonté d'organiser un vaste débat portant sur *« la collecte et l'utilisation de données biométriques*[1] *à des fins d'identification à distance »*[2]. Autrement dit, l'organe exécutif de l'Union européenne (UE) prévoit d'initier un dialogue sur le sujet des technologies de reconnaissance faciale. Selon le cadre en vigueur au sein de l'UE, le recours à ces technologies, basées sur l'intelligence artificielle et relativement intrusives, doit être exceptionnel. Conformément à l'article 9 du règlement général sur la protection des données (RGPD)[3], le traitement de données biométriques aux fins *« d'identifier une personne physique de manière unique »* est même interdit, sauf dans des cas bien précis : par exemple, si l'individu concerné a donné son consentement explicite, ou lorsque ce traitement est rendu nécessaire pour des motifs d'intérêt public majeur.[4] Malgré ces restrictions, les expérimentations et les usages des technologies de reconnaissance faciale se répandent dans plusieurs États membres, d'où la nécessité d'instaurer un dialogue au niveau européen et national.



1 Conformément à l'article 3 §13 de la Directive (UE) 2016/680 du 27 avril 2016, à l'article 4 §14 du Règlement (UE) 2016/679 du 27 avril 2016 et à l'article 3 §18 du Règlement (UE) 2018/1725 du 23 octobre 2018, les données biométriques sont *« les données à caractère personnel résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, qui permettent ou confirment son identification unique, telles que des images faciales ou des données dactyloscopiques [empreintes digitales] »*.

2 Commission européenne (2020), « Intelligence artificielle : Une approche européenne axée sur l'excellence et la confiance », Communication, COM(2020) 65 final, p. 26 : https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_fr.pdf

3 Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (ci-après Règlement général sur la protection des données ou « RGPD »), article 9.

4 Pour la liste exhaustive, voir l'article 9 §2 du RGPD.

Ces dernières années, les technologies de reconnaissance faciale ont fait leur apparition dans le quotidien des Français sous diverses formes : contrôle de sécurité aux frontières avec le dispositif PARAFE[5], déverrouillage de smartphones et applications, accès à des locaux sécurisés ou encore paiements en ligne. Des expérimentations de ces technologies à des fins sécuritaires ont également été menées, comme ce fut le cas lors du carnaval de Nice en mars 2019. Des développements similaires sont observés dans la plupart des pays européens. Bien que ces technologies jouissent désormais d'une certaine maturité et permettent dans certains cas des gains en termes de temps, de praticité voire même de sécurité, leur déploiement et leur usage, par leur recours à des données biométriques, ne sont pas sans impact sur nos droits et libertés fondamentaux. Cet impact est d'autant plus fort qu'une décision reposant sur une technologie de reconnaissance faciale peut aboutir par exemple à l'arrestation et la mise en détention d'un individu lorsque ces technologies sont utilisées à des fins sécuritaires.

Ces enjeux sont au cœur des travaux de Renaissance Numérique, qui défend la vision d'une société numérique inclusive et respectueuse des libertés et droits fondamentaux. En accord avec cette mission, le think tank demeure vigilant vis-à-vis de dispositifs numériques intrusifs et/ou susceptibles de restreindre les libertés publiques. Bien qu'elles ne reposent pas sur des technologies de reconnaissance faciale en tant que telles, les expérimentations portant sur des dispositifs de détection des masques dans le cadre de la crise sanitaire actuelle (dans la ville de Cannes[6] et à la station Châtelet-Les Halles du métro parisien[7]) témoignent d'une tendance qui doit nous préoccuper. Si le fait de disposer de solutions numériques clés-en-main pour faire face à des problèmes complexes peut sembler attrayant, il convient toutefois de ne pas se précipiter vers ces outils sans s'interroger au préalable sur leurs potentiels effets négatifs sur nos droits et libertés. La multiplication de ces tests met également en lumière un enjeu de société qui va bien au-delà des technologies de reconnaissance faciale : le recours à la vidéo intelligente dans l'espace public. Du fait de progrès technologiques importants (notamment en ma-

5 Le dispositif « Passage automatisé rapide des frontières extérieures » (PARAFE) repose sur le contrôle automatisé des passeports biométriques, soit par une analyse des empreintes digitales, soit par le recours à des technologies de reconnaissance faciale.

6 « À Cannes, des tests pour détecter automatiquement par caméras le port du masque », *Le Monde*, 28 avril 2020 : https://www.lemonde.fr/pixels/article/2020/04/28/a-cannes-des-tests-pour-detecter-automatiquement-par-cameras-le-port-du-masque_6038025_4408996.html

7 « La détection automatique du port du masque testée dans le métro parisien », *Le Parisien*, 8 mai 2020 : http://www.leparisien.fr/high-tech/la-detection-automatique-du-port-du-masque-testee-dans-le-metro-parisien-08-05-2020-8313348.php

tière d'intelligence artificielle), les dispositifs destinés à «rendre intelligents» les systèmes de vidéosurveillance connaissent des développements conséquents depuis plusieurs années. Afin de faire respecter le confinement dans le cadre de la lutte contre le Covid-19, la préfecture de police de Paris a ainsi eu recours à des drones pour surveiller la population. Le 5 mai dernier, le tribunal administratif de Paris a rejeté le recours déposé par la Ligue des droits de l'Homme (LDH) et La Quadrature du Net à l'encontre de cet usage qui, selon les plaignants, constitue une atteinte au droit à la vie privée et du droit à la protection des données personnelles[8]. Les deux associations ont fait appel de cette décision. Le 18 mai, le Conseil d'État a rendu sa décision et tranché en faveur des deux associations, considérant qu'un tel déploiement sans l'intervention préalable d'un texte réglementaire et sans avis de la Commission nationale de l'informatique et des libertés (CNIL) constituait *« une atteinte grave et manifestement illégale au droit au respect de la vie privée »*[9]. De la même façon, le débat actuel autour de la régulation des technologies de reconnaissance faciale ravive la question de l'équilibre entre plusieurs libertés fondamentales. Il est donc nécessaire de prendre le temps d'une réflexion collective éclairée.

Pour nourrir cette réflexion, Renaissance Numérique a lancé à l'automne 2019 un groupe de travail réunissant une dizaine d'experts — chercheurs, juristes et industriels[10]. Cette diversité d'acteurs lui a permis d'aborder les enjeux liés aux technologies de reconnaissance faciale non seulement d'un point de vue technique, mais également juridique et géopolitique. Un état des lieux des technologies en question et des mesures législatives les entourant au niveau national et européen a notamment été réalisé par le groupe de travail. Outre cette démarche interne, le think tank a également sollicité les différentes parties prenantes susceptibles d'apporter un retour d'expérience sur le sujet à travers la réalisation d'une série d'auditions[11] et l'organisation d'un colloque

8 « À Paris, la justice valide la surveillance du confinement par drones policiers », *Le Monde*, 6 mai 2020 : https://www.lemonde.fr/pixels/article/2020/05/06/a-paris-la-justice-valide-la-surveillance-du-confinement-par-drones-policiers_6038884_4408996.html ; « Confinement : la surveillance policière par drones dénoncée par deux associations », *Le Monde,* 4 mai 2020 : https://www.lemonde.fr/pixels/article/2020/05/04/confinement-la-surveillance-policiere-par-drones-denoncee-par-deux-associations_6038640_4408996.html

9 Conseil d'État (18 mai 2020), n°s 440442, 440445 : https://www.conseil-etat.fr/ressources/decisions-contentieuses/dernieres-decisions-importantes/conseil-d-etat-18-mai-2020-surveillance-par-drones

10 Pour la liste complète des experts membres du groupe de travail, voir la rubrique « Le groupe de travail » du présent rapport.

11 Pour la liste des personnes auditionnées, voir la rubrique « Remerciements » du présent rapport.

à l'Assemblée nationale en coopération avec Jean-Michel Mis, Député de la Loire. Plusieurs dizaines d'acteurs clés, issus du secteur public, privé et de la société civile, ont ainsi contribué à nourrir les réflexions présentées ici. Dans le souci de replacer l'intérêt général et le citoyen au cœur du débat, Renaissance Numérique a également conduit, en partenariat avec l'institut Ifop, une enquête d'opinion[12] sur la perception des Français vis-à-vis des technologies de reconnaissance faciale. Cette photographie à un instant T a confirmé la nécessité de prendre du recul sur le sujet. En effet, parmi les sondés, seuls 18% estiment être tout à fait informés sur ces technologies pour avoir un avis précis sur la manière dont elles doivent être utilisées dans la société[13]. Selon les individus interrogés, le recours à ces systèmes est surtout lié à des missions de sécurité publique : en réponse à une question ouverte, ces derniers mettent en avant les usages sécuritaires et y associent une dimension relativement anxiogène au travers des enjeux de surveillance. Ces usages ne forment pourtant qu'une partie de l'équation. Avant d'initier toute réflexion, il convient donc de définir clairement ce que sont les technologies de reconnaissance faciale.

Très concrètement, les technologies de reconnaissance faciale développées actuellement reposent sur des méthodes d'intelligence artificielle qui appliquent des techniques dites d'apprentissage profond *(deep learning)* au domaine de la vision par ordinateur, permettant de reconnaître des visages sur des images (vidéo ou fixes) en s'appuyant sur des données biométriques. Contrairement à certaines idées reçues, ces technologies ne permettent pas d'analyser les sensations ou émotions ressenties par un individu. En cela, elles diffèrent des technologies de reconnaissance comportementale ou émotionnelle, qui elles reposent notamment sur l'analyse de la coordination des mains, des tremblements, du mouvement des yeux ou encore des muscles du visage. En tant que telles, ces dernières se situent hors du champ de la présente réflexion, même si la possibilité de coupler des systèmes d'analyse comportementale avec des technologies de reconnaissance faciale soulève des questions supplémentaires et ne doit pas être ignorée. Les technologies de reconnaissance faciale ne doivent pas non plus être confondues avec la détection de visages, certes un autre pan de la vision par ordinateur mais qui ne permet pas d'associer *de facto* des visages et des individus. Enfin, il est

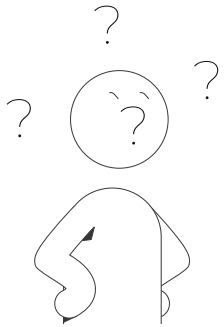
12 L'enquête, réalisée sur un échantillon de 2007 personnes, se veut représentative de la population française âgée de 18 ans et plus.

13 Pour l'analyse de cette enquête, voir Renaissance Numérique (2019), « Reconnaissance faciale : Ce que nous en disent les Français » , 6 pp. : https://www.renaissancenumerique.org/ckeditor_assets/attachments/444/rn-analyse-reconnaissancefaciale.pdf

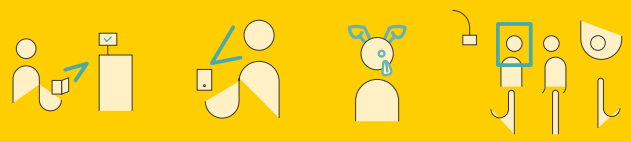
important de rappeler que tout système de vidéosurveillance n'est pas nécessairement équipé d'une technologie de reconnaissance faciale.

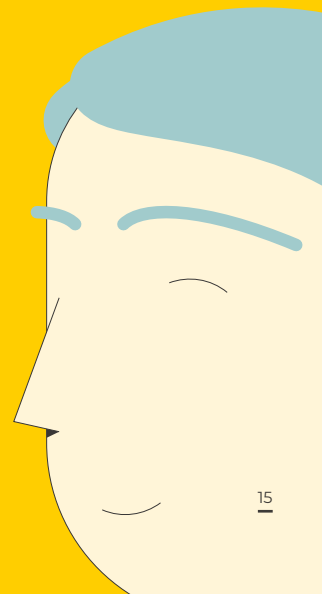
Notons également que le think tank a pris le parti d'analyser le spectre des technologies de reconnaissance faciale dans sa diversité et non « la reconnaissance faciale » en tant que concept uniforme. Aborder la reconnaissance faciale comme une technologie unidimensionnelle n'aurait pas de sens, tant les formes et les usages des technologies en question sont variés. Qui plus est, tous les usages (publics ou privés, consentis ou à l'insu des individus, en temps réel ou différé, etc.), ne comportent pas la même sensibilité et les mêmes facteurs de risque. Dès lors, se pose la question de l'adéquation du cadre réglementaire entourant ces différents usages. Le cadre juridique actuel est-il suffisant ? Faut-il le compléter en distinguant ces applications, pour le rendre plus protecteur ?

Le déploiement des technologies de reconnaissance faciale en Europe obéissant à des standards principalement américains, il convient également d'aborder ces questions sous l'angle international. La prédominance des États-Unis en la matière soulève des interrogations en termes de souveraineté numérique d'autant plus importantes, que ce sont les données personnelles des citoyens européens parmi les plus sensibles qui sont en jeu. S'interroger sur le cadre international dans lequel ces technologies sont déployées fait ressortir deux enjeux fondamentaux pour l'Union européenne : non seulement asseoir son indépendance technologique, mais également développer des technologies conformes à ses valeurs. Comme cela a été le cas dans le domaine de la protection des données personnelles avec l'avènement du RGPD, l'UE a aujourd'hui l'opportunité de s'emparer de ces questions afin de garantir la protection de ses citoyens.



PARTIE 1
LA MATURITÉ TECHNIQUE DES TECHNOLOGIES DE RECONNAISSANCE FACIALE OUVRE LA VOIE AU DÉPLOIEMENT DE LEURS USAGES





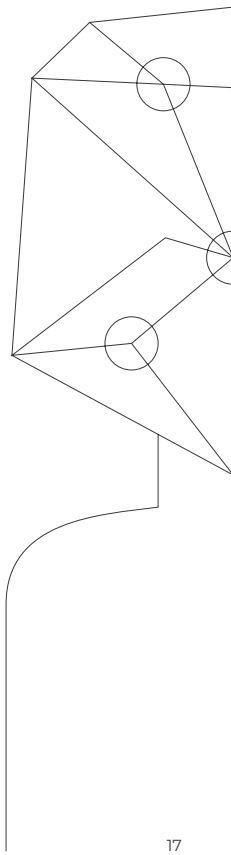
UNE MATURITÉ QUI S'INSCRIT DANS LA DYNAMIQUE DES TECHNOLOGIES D'INTELLIGENCE ARTIFICIELLE

La recherche en intelligence artificielle englobe un vaste champ de recherches fondamentales et appliquées. Le terme « intelligence » évoque des systèmes autonomes dans la prise de décision et peut donc nourrir des fantasmes selon lesquels des décisions critiques sont prises sans le consentement d'opérateurs humains. Or, les technologies de reconnaissance faciale concernent essentiellement des traitements de l'information simples à effectuer pour un cerveau biologique, mais complexes à automatiser sur des machines.

Plus précisément, les technologies de reconnaissance faciale reposent sur une application des techniques mathématiques et informatiques développées dans le domaine de la vision par ordinateur, une branche de l'intelligence artificielle. Ces techniques sont aujourd'hui étudiées sous l'approche de l'apprentissage machine *(machine learning),* un champ d'étude à la croisée de l'intelligence artificielle et de la science des données. Le plus souvent, cet apprentissage est supervisé, c'est-à-dire qu'un algorithme entraîne un modèle statistique à reconnaître des visages sur des images à partir d'une quantité massive de données (*big data*) annotées.

Les récentes recherches sur la reconnaissance faciale appliquent des méthodes d'apprentissage profond ou *deep learning* (voir l'encadré « L'apprentissage profond ») relativement matures. Avant cela, les techniques d'apprentissage pré-profond avaient mis plus de vingt ans pour améliorer la précision de 60% à 90% sur le benchmark *Labeled faces in the wild* (LFW)[14], un outil de référence pour les travaux sur la reconnaissance faciale. Les techniques de reconnaissance faciale « profondes » maintenant utilisées, appliquant plusieurs couches de traitement d'image en cascade afin d'extraire et transformer des caractéristiques physiques, ont bouleversé le domaine et ce depuis la conception du système de reconnaissance faciale Deepface[15] par Facebook en 2014. Deepface a obtenu une précision sans précédent de 97% sur le benchmark LFW. À titre de comparaison, même les meilleures techniques d'apprentissage pré-profond ne dépassent actuellement pas les 95%[16]. Inspiré par les performances remarquables des techniques d'apprentissage profond, l'état de l'art (Deepface, DeepID series[17], VGGFace[18], FaceNet[19] et VGGFace2[20]) s'est appuyé sur les architectures de réseaux de neurones convolutifs[21] profonds pour repousser la précision sur LFW à 99,8% en seulement trois ans (soit un taux d'erreur divisé par 15 par rapport à Deepface).

Ces résultats émanant d'acteurs académiques comme industriels sont souvent publiés dans des actes de conférences ou des journaux scientifiques à comité de lecture. Les codes source des algorithmes et modèles entraînés sont également ouverts (accès libre en *open source*), ce qui tend à favoriser le déploiement des technologies en question.



14 Le jeu de données *Labeled faces in the wild* regroupe plus de 13 000 photographies de visages annotées couvrant les conditions habituellement rencontrées dans la vie réelle : diversité de poses, d'éclairages, de mises au point, d'expressions faciales, d'âges, de genres, d'origines ethniques, d'accessoires, de maquillage, d'occlusions, d'arrières-plans et de qualité. Voir : Gary B. Huang, Manu Ramesh, Tamara Berg et Erik Learned-Miller (2007), « Labeled faces in the wild: A database for studying face recognition in unconstrained environments », *Technical Report 07-49*, University of Massachusetts, Amherst, 11p.

15 Yaniv Taigman, Ming Yang, Marc'Aurelio Ranzato et Lior Wolf (2014), « Deepface: Closing the gap to human-level performance in face verification », *CVPR*, pp. 1701-1708.

16 Mei Wang et Weihong Deng (2018), « Deep face recognition: A survey », 26 pp.

17 Voir : Yi Sun, Xiaogang Wang et Xiaoou Tang (2014), « Deep learning face representation from predicting 10,000 classes », *CVPR*, pp. 1891-1898 ; Yi Sun, Xiaogang Wang et Xiaoou Tang (2008), « Deeply learned face representations are sparse, selective, and robust », *perception*, 31:411-438 ; Yi Sun, Yuheng Chen, Xiaogang Wang et Xiaoou Tang (2014), « Deep learning face representation by joint identification-verification », *NIPS*, pp. 1988-1996 ; Yi Sun, Ding Liang, Xiaogang Wang et Xiaoou Tang (2015), « Deepid3: Face recognition with very deep neural networks », 5pp.

18 Omkar M. Parkhi, Andrea Vedaldi et Andrew Zisserman (2015), « Deep face recognition », *BMVC*, volume 1, p. 6.

19 Florian Schroff, Dmitry Kalenichenko et James Philbin (2015), « Facenet: A unified embedding for face recognition and clustering », *CVPR*, pp. 815-823.

20 Qiong Cao, Li Shen, Weidi Xie, Omkar M. Parkhi et Andrew Zisserman (2017), « Vggface2: A dataset for recognising faces across pose and age », 10 pp.

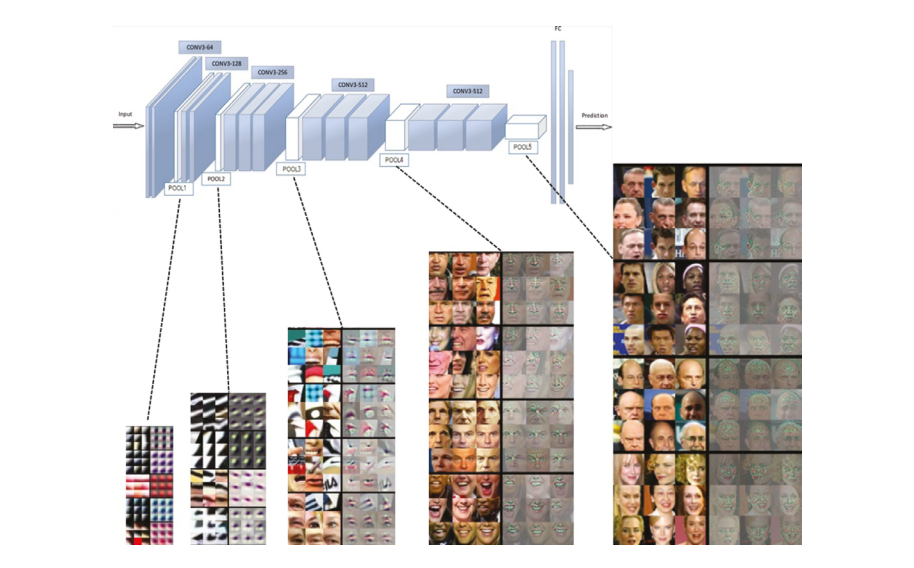
21 Un réseau de neurones artificiels convolutifs est un type de réseau de neurones artificiels dans lequel les neurones sont connectés de manière à calculer l'opération mathématique de convolution, afin de reproduire le processus biologique observé dans le cortex visuel des animaux.

L'apprentissage profond

L'apprentissage profond (*deep learning* en anglais) est basé sur l'entraînement de modèles de réseaux de neurones artificiels dits profonds[22], dont les percées en vision par ordinateur (notamment en 2012 lorsque le système AlexNet[23] a remporté la compétition ImageNet[24]) ont valu aux auteurs de ces recherches le prix Turing (équivalent du prix Nobel d'informatique) en 2018. L'apprentissage profond s'inspire du processus biologique qui amène le cerveau d'un jeune enfant à :

- apprendre à reconnaître des visages familiers en observant les visages dans plusieurs contextes ;
- rapidement extraire et mémoriser des caractéristiques physiques apparentes pertinentes à différents niveaux d'abstraction (coupe de cheveux, couleur des yeux, cicatrice, expression de sentiments, port d'accessoire, etc.) ;
- les associer à des personnes ou des groupes de personnes ;
- « généraliser » la reconnaissance de visage, autrement dit reconnaître un visage même dans des contextes inédits (nouvelle expression, éclairage coloré, changement de position/orientation, nouvelle coupe de cheveux, port de lunettes, etc.).

22 Yann LeCun, Yoshua Bengio et Geoffrey Hinton (2015), « Deep learning », *Nature 521*, pp. 436-444.
23 Alex Krizhevsky, Ilya Sutskever et Geoffrey E. Hinton (2012), « Imagenet classification with deep convolutional neural networks », *Advances in neural information processing systems*, pp. 1097-1105.
24 Jia Deng, Wei Dong, Richard Socher, Li-Jia Li, Kai Li et Li Fei-Fei (2009), « ImageNet: A Large-Scale Hierarchical Image Database », *2009 conference on Computer Vision and Pattern Recognition*.



Le schéma ci-dessus[25] présente différentes invariances et abstractions apprises par un réseau de neurones artificiels convolutifs entraîné sur une tâche de reconnaissance faciale. La première couche a appris à reconnaître automatiquement des formes certes élémentaires, mais néanmoins similaires à celles conçues manuellement par des experts humains pendant des décennies. La seconde couche a appris à identifier des textures. Les caractéristiques apprises par la troisième couche sont plus complexes : on observe des yeux, des bouches et des nez. Dans la quatrième couche, des expressions faciales sont détectables comme un sourire ou des sourcils froncés. Enfin, la dernière couche combine les caractéristiques issues des couches précédentes pour produire une représentation (une abstraction) globale du visage censée encoder suffisamment d'informations sur celui-ci pour l'identifier avec une stabilité sans précédent.

25 Ce schéma est tiré de Mei Wang et Weihong Deng (2018), *op. cit.*, p. 2.

LE CHAMP DE LA RECONNAISSANCE FACIALE REPRÉSENTE UNE DIVERSITÉ D'USAGES

L'analyse de la reconnaissance faciale ne peut s'envisager que dans la pluralité de ses applications. Il est possible de classer les tâches de reconnaissance faciale en deux catégories : la vérification (ou authentification) et l'identification (ou reconnaissance) de visage.

DES USAGES VARIÉS QUI COMPORTENT DIFFÉRENTS NIVEAUX DE RISQUES

La vérification (ou l'authentification) de visage compare une image de visage donnée à une identité connue et répond à la question « la personne figure-t-elle sur l'image ? ». La vérification, en tant que système de déverrouillage (par exemple de smartphone), est une forme de biométrie, au même titre que la reconnaissance des empreintes digitales ou de l'iris. L'identification (ou la reconnaissance) de visage associe une image de visage donnée à une identité (ou un groupe de personnes) parmi une base de données de visages connus. L'identification répond à la question « qui est cette personne ? ». Elle s'applique dans le cadre d'un système de surveillance ou de fluidification des parcours dans le monde physique (par exemple suivi de clients) ou en ligne. La détection de visage, qui permet de reconnaître la présence d'un visage sur une image et éventuellement de le segmenter ou de le suivre si l'entrée du système est une séquence d'images (par exemple une vidéo), est souvent la première étape d'un système de vérification ou d'identification. Son but est d'aligner et normaliser les visages contenus dans les images.

Les trois étapes de la reconnaissance faciale biométrique

1) Phase d'enrôlement

La première étape consiste à capturer les données suffisamment représentatives de la diversité de contextes dans lesquels les personnes cibles apparaîtront pendant l'utilisation de la technologie. Ceci correspond à une prise d'image peu contrôlée, par exemple d'individus en mouvement. Les ingénieurs peuvent également s'appuyer sur des bases de données publiques. L'entraînement des modèles d'apprentissage se fait à partir de ces bases de données.

2) Phase de stockage

Une technologie peut centraliser les photographies de ses utilisateurs sur un serveur, mais l'utilisateur peut préférer que toutes ses données biométriques personnelles soient stockées au plus près de lui, directement sur son smartphone ou sur une carte d'embarquement si l'application s'y prête. Il faut alors comparer les différents niveaux de cybersécurité entre les modes de stockage.

3) Phase de vérification

Le modèle entraîné renvoie un score d'authentification et l'application décide si ce score est suffisant pour conclure à la vérification (typiquement si ce score dépasse un seuil prédéfini). La vérification peut elle aussi avoir lieu sur un serveur ou se rapprocher au plus du capteur, du système de stockage et/ou de l'utilisateur.

Ces tâches nécessitent des systèmes de reconnaissance avec différents niveaux de précision, de sensibilité et de spécificité[26] selon leurs applications et leurs contextes d'utilisation : les performances d'un modèle utilisé à des fins de sécurité (sécurité aux frontières, déverrouillage de smartphone, paiement en ligne, accès aux services publics) sont ainsi plus critiques que celles d'un modèle consacré au marketing (publicité ciblée), lui-même plus exigent qu'une application récréative (identification sur des photographies sur un réseau social, *face swapping*).

26 « *En statistique, la sensibilité d'un test mesure sa capacité à donner un résultat positif lorsqu'une hypothèse est vérifiée. Elle s'oppose à la spécificité, qui mesure la capacité d'un test à donner un résultat négatif lorsque l'hypothèse n'est pas vérifiée* ». Définition tirée de Wikipedia : https://fr.wikipedia.org/wiki/Sensibilité_et_spécificité

L'expérience *face swap*

Développée par Snapchat depuis 2016, l'application *face swap* permet d'échanger son visage avec celui de ses amis sur une photographie ou une courte vidéo dans un but récréatif. Le déploiement de *face swap* a toutefois alimenté de nombreuses polémiques liées au risque de manipulation de l'information :

- S'agissant du détournement de l'image, *face swap* peut être détourné pour mettre en scène des individus dans des situations compromettantes, par exemple en calquant le visage d'individus sur le corps d'acteurs pour simuler la reproduction d'images ou de vidéos à caractère pornographique. Ce détournement de l'image ou *deepfake* a suscité plusieurs mesures du secteur de la pornographie. La plateforme spécialisée Pornhub s'est ainsi engagée à interdire la diffusion de *deepfakes* et rappelé la nécessité de recueillir le consentement d'individus représentés dans des vidéos à caractère pornographique avant de diffuser de tels contenus[27].

- S'agissant du détournement d'une prise de parole, *face swap* permet l'évolution dynamique d'un visage, par exemple pour faire remuer la bouche d'un individu et ainsi lui prêter des propos qu'il n'a pas tenus. En 2016, une vidéo utilisant *face swap* a ainsi mis en scène un dirigeant israélien menaçant le Pakistan. En réponse, le Ministre de la défense du Pakistan a été conduit à tenir une conférence de presse pour démentir officiellement l'existence d'une telle menace[28], qui aurait pu mener le Pakistan et Israël, tous deux puissances nucléaires, à entrer en guerre.

Les polémiques liées à l'utilisation de *face swap* n'ont pas disparu à l'heure actuelle. L'usage de ces technologies a encore été amélioré par le logiciel Zao, qui exacerbe le risque de manipulation de l'information. Par ailleurs, la question du stockage des données faciales collectées a été soulevée par bon nombre d'utilisateurs en Chine, sans qu'une réponse officielle n'ait pour l'heure été faite[29].

27 « Pornhub and Twitter ban AI-generated « deepfakes » videos that put female celebrities' faces on adult actresses' bodies », *The Independent*, 7 février 2018 : https://www.independent.co.uk/life-style/gadgets-and-tech/pornhub-twitter-deepfakes-ban-ai-celebrity-faces-porn-actress-bodies-emma-watson-jennifer-lawrence-a8199131.html

28 « Experts fear face swapping tech could start an international showdown », *The Outline*, 1 février 2018 : https://theoutline.com/post/3179/deepfake-videos-are-freaking-experts-out?zd=1&zi=4q34t-pv2

29 « Zao, l'application de vidéos «*deepfake*» qui inquiète les internautes chinois », *Le Figaro*, 2 septembre 2019 : https://www.lefigaro.fr/secteur/high-tech/vie-privee-les-videos-deepfake-de-l-application-zao-inquietent-les-internautes-chinois-20190902

À cet égard, les usages particulièrement sensibles, notamment à des fins de sécurité, nécessitent des taux d'erreur extrêmement bas. Un système déployé à l'échelle de la population de l'Union européenne devrait atteindre un taux d'erreur de 0,00000224% (soit un taux de précision de 99,99999776%) pour commettre moins de 10 erreurs sur un total de 446 millions d'individus. Nous sommes encore loin de telles performances.

Dans l'analyse des technologies de reconnaissance faciale, il faut également prendre en compte, outre leur fonction, la nature de l'utilisateur direct. Il peut en effet s'agir, entre autres, d'un individu consentant par accord préalable à l'aide de conditions générales d'utilisation (voir même de fonctionnement), d'une entreprise privée utilisant l'identification faciale dans un but commercial, ou d'un service public cherchant à surveiller une population. Dans les deux derniers cas, la reconnaissance faciale peut être appliquée à l'insu des individus ciblés et donc l'identification porte un enjeu de droit au respect de la vie privée. C'est le cas de plusieurs dispositifs de reconnaissance faciale actuellement déployés et/ou expérimentés en France par les services publics sur des enjeux régaliens :

- Le fichier de traitement des antécédents judiciaires (TAJ) est notamment utilisé à des fins d'enquêtes judiciaires ou administratives. Aux termes des articles 230-6 à 230-11 du Code de procédure pénale[30], le TAJ comprend la photographie de personnes mises en cause ou faisant l'objet d'une enquête ou d'une instruction pour recherche des causes de la mort, de blessures graves ou d'une disparition, qui comporte des caractéristiques techniques permettant de recourir à un dispositif de reconnaissance faciale. Étant donné le caractère particulièrement sensible de cet usage (il peut aboutir à une sanction pénale allant jusqu'à l'emprisonnement), le traitement des données est opéré sous le contrôle du procureur de la République territorialement compétent. Ce dernier peut ordonner l'effacement des données personnelles ayant fait l'objet d'un traitement, par exemple en cas d'acquittement ou de classement sans suite de l'enquête.

- Le système de passage rapide et sécurisé aux frontières extérieures (PARAFE) avec biométrie à reconnaissance faciale a lui été mis en place à des fins de fluidification des flux en 2018. Il permet aux passagers qui

30 Articles créés par la loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure.

y consentent de franchir la frontière française en utilisant le contrôle automatisé de leur passeport[31] par un dispositif de reconnaissance faciale. Selon Mathieu Rondel, Directeur expertise et performance opérationnelle à la Direction des opérations aéroportuaires du groupe ADP, le passage de la frontière par reconnaissance faciale prendrait 10 à 15 secondes, contre 30 secondes par reconnaissance digitale et 45 secondes par reconnaissance physique par un agent de la police aux frontières[32]. En amont du déploiement de cet usage, la question de la protection de la vie privée des voyageurs a été mise sur le devant de la scène. Saisie en 2016 sur le projet de décret visant à autoriser ces dispositifs (les portiques automatiques PARAFE reposaient jusqu'alors sur la reconnaissance des empreintes digitales), la CNIL a rappelé son opposition à la création d'une base centrale de données qui permettrait d'identifier les personnes[33]. Selon la Commission, le recours au passeport biométrique, qui permet de conserver les données personnelles des individus sur *« un support dont la personne a l'usage exclusif »*, est *« de nature à assurer une meilleure protection de la vie privée des personnes »*[34]. Cette recommandation est aujourd'hui appliquée. Les portiques ne sont par ailleurs accessibles qu'aux individus âgés de 12 ans et plus et leur utilisation est facultative, puisque la possibilité de se présenter devant un agent de la police aux frontières demeure. L'existence de cette alternative est considérée comme une garantie supplémentaire par la CNIL.

- Enfin, l'authentification en ligne certifiée sur mobile (ALICEM), à des fins d'accès aux services publics est actuellement expérimentée en France. Il s'agit d'une application développée par le Ministère de l'Intérieur et l'Agence nationale des titres sécurisés (ANTS) qui donne accès à l'ensemble des services partenaires de FranceConnect, le dispositif de l'État qui facilite l'accès aux services en ligne et compte plus de 500 services publics disponibles. Lors de la création d'un compte sur ALICEM par un individu, la photo contenue sur la puce de son titre d'identité (passeport ou titre de séjour biométrique) est extraite par lecture sans contact. Le particulier est ensuite invité à réaliser une vidéo en temps réel (en mode « selfie ») et doit effectuer trois actions (à savoir, sourire, tourner la tête et cligner des yeux, suivant un ordre aléatoire). Une reconnaissance faciale dite « statique » est également réalisée à partir d'une photographie extraite de la vidéo et comparée à celle conservée dans la puce du titre. Comme les deux exemples précédents, cette application soulève des questions en termes de protection des données personnelles auxquelles l'État tente de répondre. Le Ministère de l'Intérieur a ainsi fait savoir que les données personnelles des utilisateurs ne sont stockées que sur les smartphones de ces derniers et ne sont utilisées par ALICEM que lors de l'inscription au dispositif[35]. Le ministère précise également que ces données *« ne font l'objet d'aucune utilisation pour d'autres objectifs que l'authentification électronique et l'accès à des services en ligne par ALICEM »* et qu'elles ne sont pas transmises à des tiers.[36] Saisie pour avis sur le projet de décret mettant en place le traitement de données biométriques dans le cadre du développement de l'application, la CNIL a – par délibération du 18 octobre 2018[37] – notamment considéré que la mise en œuvre de cette application devait être subordonnée au développement de solutions alternatives aux technologies de reconnaissance faciale, afin de s'assurer de la liberté effective du consentement des personnes au traitement de leurs données biométriques au moment de l'activation de leur compte.

31 Décret n° 2016-414 du 6 avril 2016 portant modification d'un traitement automatisé de données à caractère personnel dénommé « PARAFE ».
32 Renaissance Numérique (2019), « Reconnaissance faciale : Interdiction, expérimentation, généralisation, réglementation. Où en est-on ? Où allons-nous ? », p. 19 : https://www.renaissancenumerique.org/publications/reconnaissance-faciale-interdiction-experimentation-generalisation-reglementation-ou-en-est-on-ou-allons-nous. Voir également à ce sujet la publication du Groupe ADP sur Twitter, en date du 6 juillet 2018 : https://twitter.com/GroupeADP/status/1015124993729015808
33 Délibération n° 2016-012 du 28 janvier 2016 portant avis sur un projet de décret portant modification d'un traitement automatisé de données à caractère personnel dénommé PARAFE : https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000032372514&categorieLien=id
34 *Ibid.*

35 Ministère de l'Intérieur, « Alicem, la première solution d'identité numérique régalienne sécurisée », 16 décembre 2019 : https://www.interieur.gouv.fr/Actualites/L-actu-du-Ministere/Alicem-la-premiere-solution-d-identite-numerique-regalienne-securisee
36 *Ibid.*
37 Délibération n° 2018-342 du 18 octobre 2018 portant avis sur projet de décret autorisant la création d'un traitement automatisé permettant d'authentifier une identité numérique par voie électronique dénommé « Application de lecture de l'identité d'un citoyen en mobilité » (ALICEM) et modifiant le code de l'entrée et du séjour des étrangers et du droit d'asile demande d'avis n° 18008244 : https://www.legifrance.gouv.fr/jo_pdf.do?id=JORFTEXT000038475742

La reconnaissance faciale appliquée à des fins sécuritaires à l'international

La Chine utilise ces technologies à des fins de contrôle social des individus et de profilage racial des Ouïghours, dans une logique de surveillance politique.

Aux États-Unis, malgré des initiatives conduites par certains États pour interdire ces technologies, la reconnaissance faciale est employée par des agences fédérales à des fins de garantie de la sécurité nationale. En juin 2019, le Congrès américain a souligné dans un rapport les efforts conduits par le FBI et le Département de la Justice pour encadrer l'utilisation de technologies de reconnaissance faciale, depuis ses précédentes recommandations émises en 2016. Il regrette toutefois que la plupart de ses recommandations n'aient pas été suivies et insiste sur la nécessité d'actualiser les lignes directrices en matière de protection des données collectées par ces technologies, préalablement au déclenchement de projets pilotes[38].

Singapour procède à la sécurisation à l'aéroport de Changi par le biais de dispositifs analogues au mécanisme PARAFE, qui utilisent des technologies de reconnaissance faciale[39].

Le Royaume-Uni est l'un des seuls États membres de l'OCDE à utiliser la reconnaissance faciale en public à partir de bases de données, sans passer par des tests. Les technologies déployées reposent sur le fonctionnement suivant : des images numériques de visages de passants sont prises à partir de flux vidéo en direct et traitées en temps réel pour extraire des informations biométriques faciales. Ces informations sont ensuite comparées aux informations biométriques faciales des personnes figurant sur des listes de surveillance préparées spécifiquement aux fins de chaque déploiement.

38 United States Government Accountability Office (2019), « Face Recognition Technology: DOJ and FBI Have Taken Some Actions in Response to GAO Recommendations to Ensure Privacy and Accuracy, But Additional Work Remains », 23 pp.

39 « Singapore is introducing facial recognition at Tuas checkpoint. But there is one major drawback », *Mashable SE Asia*, avril 2019 : https://sea.mashable.com/tech/3231/singapore-is-introducing-facial-recognition-at-tuas-checkpoint-but-there-is-one-major-drawback

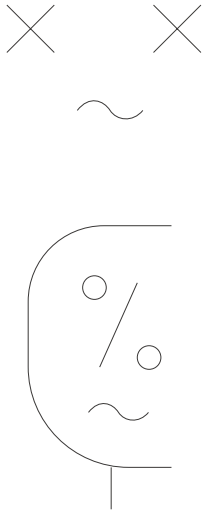
LE CHEVAUCHEMENT AVEC D'AUTRES TECHNOLOGIES SOULÈVE ÉGALEMENT DES INTERROGATIONS

Le règlement général sur la protection des données (RGPD) consacre la nécessité d'effectuer une analyse d'impact relative à la protection des données (AIPD), obligatoire lorsque les traitements visent à identifier des personnes physiques de manière unique parmi lesquelles figurent des personnes dites « vulnérables » (par exemple élèves, personnes âgées, patients, demandeurs d'asile, etc.).

Bien qu'une technologie de reconnaissance faciale puisse être employée pour un usage acceptable, une analyse fine du contexte dans lequel celle-ci est déployée peut prévenir les risques soulevés par sa combinaison avec d'autres technologies afin d'améliorer les fonctions d'identification et de reconnaissance d'individus. Par exemple, un système de reconnaissance faciale couplé à un système de reconnaissance des empreintes digitales, de l'iris ou encore comportementale, peut accroître, sinon créer de nouveaux risques de violation du consentement des individus et de leur droit au respect de la vie privée. En effet, il se peut que le recoupement de diverses bases de données génère de nouvelles données personnelles sans l'accord des utilisateurs.

L'usage d'une application pouvant en amener un autre, il est également crucial d'évaluer la technologie et son impact non seulement au moment du déploiement initial, mais aussi dans la durée, afin d'évaluer les risques futurs. À ce titre, se pose la question de la responsabilité lorsqu'une application combine les technologies de plusieurs acteurs.

Enfin, la métrique servant à mesurer la performance des algorithmes n'est pas absolue et doit dépendre du contexte dans lequel un algorithme est utilisé et de son éventuel couplage à d'autres technologies biométriques : par exemple, une décision de justice en appel peut minimiser les erreurs de type I (faux positifs), alors que les premières étapes d'une enquête anti-terroriste cherchent à réduire les erreurs de type II (faux négatifs).



DES TECHNOLOGIES QUI NE SONT PAS INFAILLIBLES

LES LACUNES INHÉRENTES DES TECHNOLOGIES DE RECONNAISSANCE FACIALE

Le National Institute of Standards and Technology (NIST), une agence du département du Commerce des États-Unis chargée, entre autres, d'évaluer des algorithmes et de définir des standards, a publié en 2018 la partie 1 du rapport *« Ongoing Face Recognition Vendor Test »* (FRVT). Cette étude compare les performances de 127 algorithmes d'identification de visages soumis par 45 laboratoires industriels et commerciaux de recherche et développement (dont l'allemand Cognitec, l'américain Microsoft, le chinois Yitu, le français IDEMIA, le japonais NEC et le russe VisionLabs) et une université, sur un jeu de données de 26,6 millions de portraits contrôlés représentant 12,3 millions d'individus. Malgré des approches et des performances différentes, les meilleurs algorithmes atteignent en 2018 des taux d'erreur inférieurs à 0,2%. Néanmoins, pour au moins 10% des images, même si l'identification réussit, le taux de confiance[40] est bas et une décision humaine reste indispensable pour écarter l'hypothèse que l'identité proposée soit un faux positif.

40 Le taux de confiance d'une prédiction algorithmique indique le degré auquel un algorithme est sûr du résultat qu'il propose. Il est parfois appelé « score d'authentification » pour la reconnaissance faciale et s'exprime en général sous la forme d'une probabilité. *« Par exemple, un système de détection des visages peut prédire qu'une région d'image est un visage à un score de confiance de 90 %, et qu'une autre région d'image est un visage à un score de confiance de 60 %. »* (Amazon Web Services (2020), « Amazon Rekognition : Manuel du développeur », p.132).

La qualité de la capture d'image

Les problèmes de qualité d'image proviennent du système de capture d'image (caméra), de l'environnement (lumière) ou de la présentation du visage au système de capture (orientation, occultation). Les problèmes liés au système de capture d'image et, dans une certaine mesure, ceux causés par l'environnement sont extrinsèques à la technologie logicielle de reconnaissance faciale et seront sans doute résolus par de meilleurs systèmes de capture et traitement de l'image. Ce sont d'ailleurs ces problèmes de qualité qui ont été mis en cause pour expliquer la valeur prédictive positive très faible (8%) observée lorsqu'un système de reconnaissance faciale a été utilisé lors de la finale de la Ligue des Champions en 2017 à Cardiff pour détecter la présence d'éventuels criminels[41].

L'émergence et la combinaison d'algorithmes efficaces, de ressources informatiques puissantes et de jeux de données annotées massives ont permis d'améliorer les performances de la reconnaissance faciale au point de rendre ces technologies accessibles pour des utilisations pratiques et commerciales. Nous pouvons raisonnablement nous attendre à continuer de voir décroître vers zéro le taux d'erreur sur des jeux de données déterminés. Néanmoins, au fur et à mesure que des hypothèses idéales deviennent obsolètes (éclairage moins optimal, position moins adéquate, etc.), d'autres défis et problématiques apparaissent lorsque ces algorithmes sortent des laboratoires de recherche et sont intégrés à des applications courantes.

Notons d'abord que les problèmes de ressemblance de visages font croître le taux d'erreur à mesure que la population considérée augmente : il est multiplié par 1,6 en considérant une population de 12 millions d'adultes par rapport à une population de 640 000 adultes. En plus des sosies, les algorithmes testés par le NIST sont incapables de distinguer des jumeaux, qu'ils soient monozygotes (« vrais jumeaux ») ou dizygotes (« faux jumeaux »). Le rapport de l'agence américaine mentionne aussi de mauvaises performances lorsqu'il s'agit d'identifier des individus au fil du temps. Alors que les systèmes n'ont pas de mal à reconnaître un individu si on leur présente une photo de ce der-

41 À ce sujet, voir le site dédié aux dispositifs de reconnaissance faciale automatique développé par la *South Wales Police* : http://afr.south-wales.police.uk/

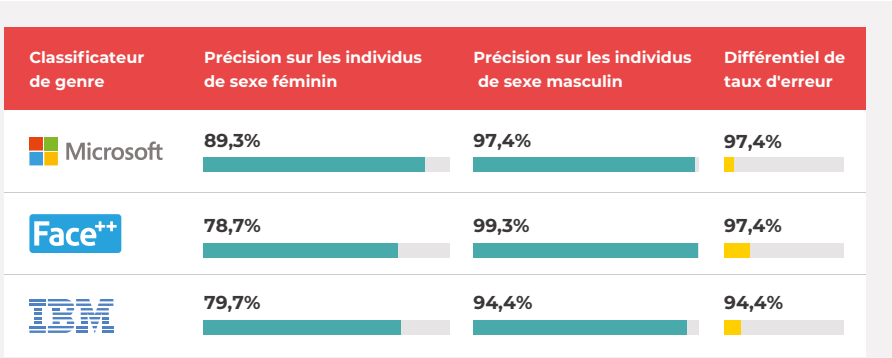
nier ayant vieilli de deux ans (ou « photo à + 2 ans »), il en va tout autrement si on leur présente une photo du même individu ayant vieilli de dix-huit ans (ou « photo à +18 ans »). Même pour le meilleur système testé, le taux d'erreur sur des photos d'adultes ayant vieilli de 18 ans est multiplié par cinq par rapport à celui observé sur les photos d'individus ayant vieilli de seulement deux ans. Les systèmes, et particulièrement ceux destinés aux applications judiciaires s'inscrivant dans le temps, doivent intégrer les évolutions physiques des individus liées à l'âge, mais aussi les facteurs qui peuvent les accélérer (consommation de médicaments ou de drogues) ou les ralentir (chirurgie esthétique).

Plus grave encore, des études ont montré que certaines technologies de reconnaissance faciale causent des biais pouvant provoquer des discriminations racistes, sexistes ou âgistes. Ces biais proviennent principalement des données sur lesquelles les modèles d'apprentissage sont entraînés. En effet, les bases de données publiques comme VGGFace2 (visages issus de Google Images) et MS-Celeb-1M[42] (visages de célébrités) proviennent souvent de sites web et collectent des photographies avantageuses de célébrités jeunes, souriantes et maquillées. Ces photographies généralisent ainsi mal la physionomie des populations au quotidien. Cependant, même une base de données créée à partir d'images de la vie quotidienne peut montrer une distribution inégale des différents attributs physiques d'une population. D'abord, un groupe (pas forcément minoritaire) peut être sous-représenté dans cette base de données à cause d'un défaut de représentativité dans la création même de la base de données, par exemple si celle-ci est générée à partir d'un échantillon où les hommes sont plus nombreux que les femmes. Toutefois, même une base de données ayant une distribution fidèle à celle de la population ciblée collecte moins d'exemples représentant un groupe minoritaire qu'un groupe majoritaire et peut entraîner les modèles à produire un taux d'erreur plus fort sur le groupe minoritaire que sur le groupe majoritaire, entraînant un biais et une éventuelle discrimination envers l'un des deux groupes selon l'application. Ainsi, IBM a montré que parmi les bases de données les plus utilisées pour entraîner des algorithmes de reconnaissance faciale, LFW contenait plus de 80% de photos de personnes à peau claire.

42 Yandong Guo, Lei Zhang, Yuxiao Hu, Xiaodong He et Jianfeng Gao (2016), « Ms-celeb-1m: A dataset and benchmark for large-scale face recognition », *ECCV*, pp. 87-102, *Springer*.

Ceci a poussé des chercheurs à créer des jeux de données plus diversifiés (comme par exemple *Racial Faces in-the-Wild*[43] (RFW)), afin de mesurer les biais ethniques et genrés des algorithmes de reconnaissance faciale. Même si les études sur ce sujet ne sont pas toutes consensuelles (voir la polémique sur Amazon Rekognition entre l'Union américaine pour les libertés civiles[44] et Amazon[45]), nous pouvons citer les travaux du projet *Gender shades*[46] porté par la chercheuse Joy Buolamwini au Massachusetts Institute of Technology (MIT). Cette étude a créé un jeu de données annotées, puis a testé les systèmes de reconnaissance faciale de Microsoft, IBM et Face++. Les résultats sont catégoriques : si le taux d'erreur de ces trois systèmes est inférieur à 1% pour des hommes à peau claire, il atteint plus de 20% pour des femmes à peau sombre.

GRAPHIQUE 1 - TAUX D'ERREURS OBSERVÉS SUR LES SYSTÈMES DE RECONNAISSANCE FACIALE DE MICROSOFT, IBM ET FACE++ SELON LE GENRE[47]



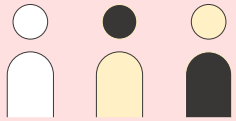
43 Mei Wang, Weihong Deng, Jiani Hu, Xunqiang Tao et Yaohai Huang (2018), « Racial faces in-the-wild: Reducing racial bias by deep unsupervised domain adaptation », 11pp.
44 « Amazon's Face Recognition Falsely Matched 28 Members of Congress With Mugshots », *American Civil Liberties Union*, 26 juillet 2018 : https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28
45 « Thoughts on Recent Research Paper and Associated Article on Amazon Rekognition », Amazon, *AWS Machine Learning Blog*, 26 janvier 2019 : https://aws.amazon.com/fr/blogs/machine-learning/thoughts-on-recent-research-paper-and-associated-article-on-amazon-rekognition/
46 Voir le site : http://gendershades.org/ et Joy Buolamwini et Timnit Gebru (2018), « Gender shades: Intersectional accuracy disparities in commercial gender classification », *Conference on Fairness, Accountability and Transparency*, pp 77-91.
47 Source : http://gendershades.org/overview.html

Ces résultats sont corroborés par une évaluation de 14 modèles commerciaux de reconnaissance faciale sur RFW qui a montré des disparités de performance entre différentes ethnies, avec une différence de taux d'erreur de 12% entre les groupes produisant les meilleures et les pires performances.

Des suspicions de biais discriminatoires médiatisées

En 2015, l'ingénieur Jacky Alciné a rendu public sur Twitter un biais existant dans Google Photo, qui détectait des gorilles sur une photographie présentant deux visages de personnes de couleur[48].

Le système d'authentification faciale d'Apple a lui aussi été accusé en 2017 dans un article du *Sun*[49] de ne pas différencier des visages de personnes d'origine asiatique aussi bien qu'il différencie ceux de personnes d'origine caucasienne.



Des études ont également montré que nonobstant des taux d'erreur très bas sur des bases de données de visages suffisamment variées, les systèmes de reconnaissance faciale sont sujets à des failles de sécurité importantes. Des attaques de présentation[50] permettent à des individus de se grimer (maquillage, masques anti-pollution comme lors des manifestations de 2019 à Hong Kong, postiches, masques 3D en silicone) pour tromper les modèles.

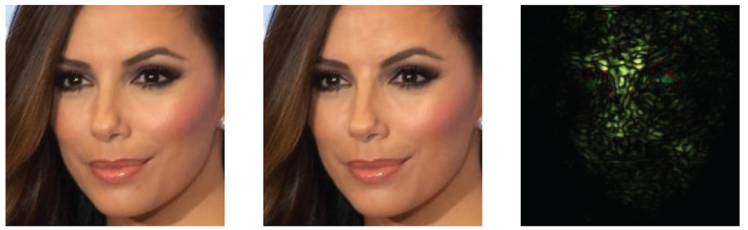
48 Voir : https://twitter.com/jackyalcine/status/615329515909156865

49 « Chinese users claim iPhoneX face recognition can't tell them apart », *The Sun*, 21 Décembre 2017 : https://www.thesun.co.uk/news/5182512/chinese-users-claim-iphonex-face-recognition-cant-tell-them-apart/

50 Raghavendra Ramachandra et Christoph Busch, « Presentation attack detection methods for face recognition systems: a comprehensive survey », *ACM Computing Surveys (CSUR)*, 50(1):8, 2017.

Les attaques par leurre

Les attaques dites « adversarielles »[51] s'appuient sur des variations subtiles, calculées et souvent imperceptibles à l'œil nu des pixels des images pour changer et fausser la prédiction des algorithmes. L'image ci-dessous en est un exemple.



Les photographies ci-dessus[52] illustrent un exemple d'attaque adversarielle. À gauche : photographie originale de l'actrice Eva Longoria. Au centre : image perturbée de l'actrice. À droite : filtre ayant perturbé l'image originale pour donner l'image perturbée. Un algorithme qui reconnaissait bien l'actrice sur la photographie de gauche a échoué à la reconnaître sur l'image perturbée au centre, alors que la perturbation nous est imperceptible à l'œil nu.

Si certains cyber-risques s'expliquent par les limites techniques de la reconnaissance faciale en tant que telle, d'autres découlent de la capacité de prédiction des algorithmes. Cette capacité de prédiction peut en outre causer des questions du point de vue éthique. Une étude parue dans *Nature Me-*

51 Akhil Goel, Anirudh Singh, Akshay Agarwal, Mayank Vatsa et Richa Singh (2018), « Unravelling robustness of deep learning based face recognition against adversarial attacks », 8 pp ; Akhil Goel, Anirudh Singh, Akshay Agarwal, Mayank Vatsa et Richa Singh (2018), « Smartbox: Benchmarking adversarial detection and mitigation algorithms for face recognition », *IEEE BTAS*, 7 pp.

52 Ces photographies sont tirées de Mahmood Sharif, Sruti Bhagavatula, Lujo Bauer, Michael K. Reiter (2016), «Accessorize to a crime: Real and stealthy attacks on state-of-the-art face recognition», *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, pp. 1528-1540.

dicine[53] a prouvé que les images de visages comportent suffisamment d'informations pour qu'un système performant puisse prédire des informations démographiques et phénotypiques comme l'expression de genre, l'âge ou des informations génétiques privées et particulièrement sensibles (liens de parentés, origines ethniques). Dans la même veine, une équipe de recherche de l'université de Stanford[54] a montré qu'un algorithme entraîné à classifier l'orientation sexuelle de femmes et d'hommes simplement à partir de caractéristiques faciales, peut prédire avec une précision de plus de 83% l'orientation sexuelle des individus, là où des humains ne dépassent pas 61%. Cette étude conclut sur les dangers de la reconnaissance faciale sur la vie privée et la sécurité des personnes LGBTQ+. Par conséquent, il est nécessaire de réfléchir aux garanties de confidentialité de ces données biologiques et de prévenir les fuites possibles. Comme le souligne Raphaël de Cormis, Vice-président Innovation et Transformation numérique chez Thalès, *« plus les données sont importantes, plus la taille du pot de miel (honeypot) peut attirer des attaquants et mettre à risque des utilisateurs »*[55]. Il convient à ce titre de se prémunir d'une centralisation des données.

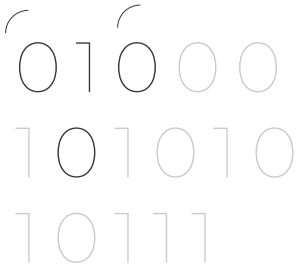
Selon le rapport du NIST, la révolution occasionnée par l'apprentissage profond explique les fortes améliorations de performance sur la période 2013-2018 comparées à celles de la période 2010-2013. En effet, les modèles de réseaux de neurones artificiels convolutifs bénéficient d'une forte robustesse aux invariances et œuvrent à la résolution des limitations dues aux présentations non contrôlées de visages devant l'objectif. Cependant, ces technologies d'apprentissage profond ne sont pas à l'abri de produire des biais discriminatoires. Or, leur aspect « boîte noire » complique leur auditabilité : il est impossible de prédire le comportement exact d'une technologie de cette nature dès sa conception. Dès lors, les acteurs de la reconnaissance faciale doivent assurer la transparence des performances de leurs modèles sur différents groupes de personnes.

53 Yaron Gurovich, Yair Hanani, Omri Bar et al. (2019), « Identifying facial phenotypes of genetic disorders using deep learning », *Nature Medicine*, 25:60 – 64.
54 Michal Kosinski et Yilun Wang (2018), « Deep neural networks are more accurate than humans at detecting sexual orientation from facial images », *Journal of Personality and Social Psychology*, Volume 114, Numéro 2, pp. 246-257.
55 Renaissance Numérique (2019), « Reconnaissance faciale : Interdiction, expérimentation, généralisation, réglementation. Où en est-on ? Où allons-nous ? », p. 34 : https://www.renaissancenumerique.org/publications/reconnaissance-faciale-interdiction-experimentation-generalisation-reglementation-ou-en-est-on-ou-allons-nous.

UNE COURSE TECHNOLOGIQUE PERPÉTUELLE POUR CORRIGER LEURS EFFETS NÉGATIFS

La révolution de l'apprentissage profond en vision par ordinateur explique les progrès récents de la reconnaissance faciale et son intégration dans des applications récréatives, commerciales, industrielles, judiciaires et sécuritaires. Les taux d'erreurs sur certaines bases de données ne cessent de diminuer (en moyenne le taux d'erreurs est divisé par 2 tous les ans). Toutefois, les jeux de données annotés qui servent à entraîner et évaluer les modèles ne sont pas toujours suffisamment divers et peuvent être à l'origine de biais qui se traduiront par des discriminations dans leurs applications. La course technologique incite donc les acteurs à minimiser les biais, soit en diversifiant les bases de données d'entraînement des modèles (par exemple en y insérant des images de synthèse), soit en améliorant les modèles eux-mêmes (par exemple en adaptant leurs capacités de reconnaissance sur les groupes majoritaires aux groupes minoritaires).

Malgré ces avancées, la course technologique pour corriger les erreurs des dispositifs de reconnaissance faciale est sans fin. D'une part, car ces technologies ne pourront par définition jamais être fiables à 100%. D'autre part, car les cyberattaques et les leurres progressent en parallèle des progrès réalisés par l'industrie.

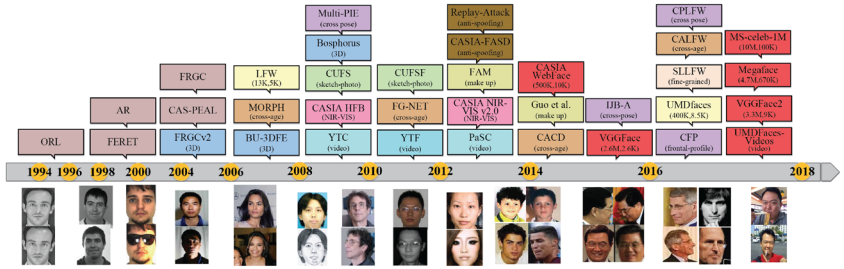


Des jeux de données d'images de visages annotées de moins en moins contrôlées

Un modèle d'apprentissage supervisé nécessite une quantité importante de données annotées pour bien apprendre et bien généraliser. Si initialement les jeux de données pour la reconnaissance faciale profonde des entreprises étaient privés, d'autres bases de données ont été rendues publiques afin que la communauté académique rattrape la recherche industrielle.

La figure ci-dessous montre l'évolution des jeux de données utilisés dans le cadre de la reconnaissance faciale, avec un effet d'échelle croissant et une généralisation des images montrant des visages avec de moins en moins de contrôle et de contraintes : les âges, les poses et les expressions varient, puis des éléments externes occultent certaines parties des visages, les rognent ou les maquillent.

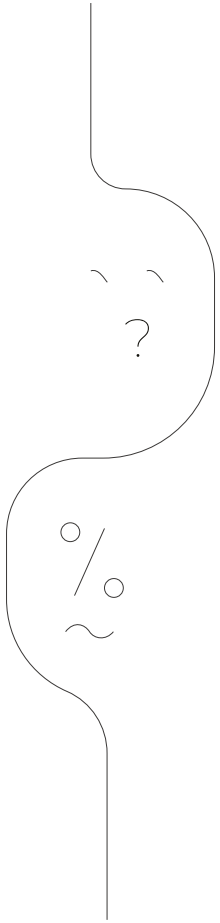
Évolution des bases de données de reconnaissance faciale depuis 1994[56]



56 Ce schéma est tiré de Mei Wang et Weihong Deng (2018), *op. cit.*, p. 13.

LES LACUNES HUMAINES FACE À UNE TECHNOLOGIE PROBABILISTE

Au-delà des lacunes d'ordre technique inhérentes aux technologies de reconnaissance faciale (erreurs, biais discriminatoires, cyber-risques), certaines failles peuvent résulter de l'intervention humaine dans les processus d'identification.



La sécurité publique est un cas d'usage typique où la décision finale revient à l'humain, les décisions en jeu étant susceptibles d'affecter gravement les libertés fondamentales des individus. Lorsqu'un système de vidéosurveillance à l'entrée d'un stade ou dans la rue identifie une personne comme étant un criminel recherché, cette identification ne saurait être automatiquement considérée comme valide. La reconnaissance faciale étant une technologie probabiliste, le risque de faux positif est, lorsqu'il s'agit d'appréhender une personne et de la mettre en état d'arrestation, beaucoup trop élevé. Dès lors, il est primordial que les agents chargés de la sécurité, et plus globalement l'ensemble des utilisateurs, soient formés à l'usage de ces technologies probabilistes et à l'interprétation des résultats présentés par ces dernières. Tout utilisateur doit se prémunir contre le « biais d'automation », qui est le fait d'accorder une confiance exagérée à la machine et d'ignorer des informations extérieures qui pourraient venir contredire les résultats de l'algorithme[57]. Afin de réduire au maximum

57 À propos du biais d'automation, voir : https://en.wikipedia.org/wiki/Automation_bias

le risque d'erreur de jugement lors de la vérification « manuelle » d'une correspondance établie par ordinateur, il est en outre indispensable de s'assurer que le taux de confiance du résultat soit le plus haut possible. Ainsi, dans son *« Manuel du développeur »* pour son produit Rekognition, Amazon conseille aux organismes chargés de l'application de la loi d'utiliser un seuil de similitude de 99% et plus[58], afin de minimiser le risque d'erreur d'identification. Comme indiqué par le manuel, une correspondance faciale établie par un système comme Amazon Rekognition, ne saurait par ailleurs constituer une preuve irréfutable de l'identité d'une personne, et doit inévitablement être corroborée d'éléments de preuve supplémentaires (vérification des documents d'identité, des empreintes digitales, de l'ADN, etc.).

Par ailleurs, il est important de considérer que toute décision prise dans laquelle une technologie de reconnaissance faciale est impliquée est le résultat d'une chaîne d'événements. Dès lors, il est indispensable d'assurer l'explicabilité des décisions à chaque niveau de la chaîne, jusqu'à la décision humaine. Or, comme le souligne la Commission européenne dans son livre blanc sur l'intelligence artificielle, *« l'opacité (« effet de boîte noire »), la complexité, l'imprévisibilité et le comportement partiellement autonome »* sont des *« particularités qui caractérisent de nombreuses technologies de l'IA »*[59]. Il ne s'agit donc pas d'expliquer comment ces « boîtes noires » fonctionnent, mais plutôt, en amont, de pouvoir identifier les données qui ont été utilisées pour faire apprendre le système et expliquer la démarche d'entraînement de ce dernier, et en aval les éléments qui ont mené le système à une décision. La compréhension en amont devrait ainsi favoriser le développement de technologies de reconnaissance faciale éthiques *by design* (c'est-à-dire dont le code source intègre des dimensions éthiques) et d'identifier dès la conception les éventuels biais inhérents à ces technologies. En aval, il s'agit de suivre dans le temps les résultats présentés par les algorithmes[60]. Le caractère évolutif de ces technologies nécessite en effet de contrôler les résultats régulièrement, afin de pouvoir les améliorer[61].

58 Amazon Web Services (2020), *Ibid.*, p.167 : https://docs.aws.amazon.com/fr_fr/rekognition/latest/dg/rekognition-dg.pdf

59 Commission européenne (2020), « Intelligence artificielle : Une approche européenne axée sur l'excellence et la confiance », Communication, COM(2020) 65 final, p. 14 : https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_fr.pdf

60 À ce sujet, voir Renaissance Numérique (2017), « L'éthique dans l'emploi à l'ère de l'intelligence artificielle », 23 pp. : https://www.renaissancenumerique.org/system/attach_files/files/000/000/137/original/Renaissance_Nume%CC%81rique_IA___Emploi_Oct2017.pdf?1508946963

61 *Ibid.*, pp. 20-21.

Par ailleurs, lorsqu'un individu se retrouve privé de sa liberté du fait d'une décision prise à l'aide d'un dispositif de reconnaissance faciale, ce n'est pas uniquement à cause de la machine. Dans les cas d'usage pour lesquels cette technologie constitue une aide à la décision, il convient également de prendre en compte les biais humains qui, peu importe le taux de confiance émis par les dispositifs, persistent. En outre, il devrait être de la responsabilité du fournisseur de la technologie de reconnaissance faciale d'expliquer à son client (par exemple les forces de l'ordre) le fonctionnement précis de ce dispositif et comment appréhender les résultats de la technologie dans sa décision. Il devrait également toujours considérer les éventuelles alternatives moins intrusives.

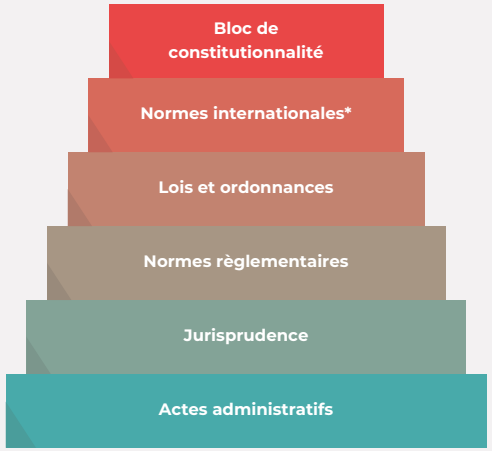
> Malgré des avancées technologiques significatives rendues possibles par le recours à l'apprentissage profond ces dernières années, les technologies de reconnaissance faciale restent des dispositifs non seulement imparfaits mais avant tout hautement sensibles. Le traitement de données biométriques est loin d'être une activité anodine et le risque de violation de nos droits et libertés fondamentaux mérite une attention particulière. Pour autant, les cas d'usages plus ou moins sensibles et les expérimentations se multiplient, et ce y compris dans plusieurs États membres de l'Union européenne. Dès lors, il est nécessaire de se demander si le cadre juridique qui les entoure peut suffire à prévenir des usages des technologies de reconnaissance faciale qui risqueraient de mettre en péril nos droits fondamentaux.

PARTIE 2
UN CADRE JURIDIQUE À L'APPLICATION DISPARATE ET PEU EFFICIENTE

LES TECHNOLOGIES DE RECONNAISSANCE FACIALE : DES DISPOSITIFS RELATIVEMENT BIEN ENCADRÉS JURIDIQUEMENT

Que ce soit en France, au sein de l'Union européenne ou au niveau international, le développement des technologies de reconnaissance faciale ne se fait pas dans un total vide juridique. Il est encadré par de nombreuses normes de divers niveaux, allant des droits et libertés fondamentaux aux législations nationales. Pour analyser le cadre juridique applicable aux technologies de reconnaissance faciale, il est donc nécessaire d'envisager l'ensemble du cadre normatif existant et de commencer par les normes supérieures, en particulier les droits et principes fondamentaux, socle des démocraties, avant de s'intéresser aux normes inférieures.

GRAPHIQUE 2 - LA HIÉRARCHIE DES NORMES



*sous réserve de ratification par les États et d'insertion dans leur système normatif

LES DROITS FONDAMENTAUX APPLICABLES AUX TECHNOLOGIES DE RECONNAISSANCE FACIALE

Les droits fondamentaux sont la base des démocraties. De fait, ils constituent également les plus hautes normes s'appliquant aux technologies de reconnaissance faciale. Au niveau international, de nombreux textes consacrent des droits fondamentaux susceptibles d'être impactés par l'utilisation de ces technologies.

DES DROITS TRÈS LARGEMENT CONSACRÉS

À cet égard, la Déclaration universelle des droits de l'homme de 1948[62] va jusqu'à relier directement les droits fondamentaux à la paix dans le monde : « *la reconnaissance de la dignité inhérente à tous les membres de la famille humaine et de leurs droits égaux et inaliénables constitue le fondement de la liberté, de la justice et de la paix dans le monde* ». Cette Déclaration est complétée au niveau international par des textes spécifiques qui précisent ou déclinent certains droits et principes contenus dans la Déclaration. C'est le cas, par exemple, du Pacte international relatif aux droits civils et politiques[63], du Pacte international relatif aux droits économiques, sociaux et culturels[64] ou encore, de la Convention relative aux droits de l'enfant[65]. L'application de ces textes internationaux dépend essentiellement de leur ratification par les États, de l'absence de réserves, et de leur intégration au niveau national (modification de la Constitution, par exemple).

Par ailleurs, les principes contenus dans la Déclaration universelle des droits de l'homme ont trouvé une nouvelle portée juridique par l'adoption au niveau régional de textes ayant force contraignante. Ainsi en est-il de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales[66] signée au sein du Conseil de l'Europe le 4 novembre 1950 et entrée en vigueur en 1953. La Cour européenne des droits de l'homme, qui siège à Strasbourg depuis 1959, veille à son application par les pays membres et au respect des droits qu'elle garantit. Au sein de l'Union européenne, le traité de Lisbonne qui est entré en vigueur le 1er décembre 2009 a conféré à la Charte des droits fondamentaux de l'Union européenne[67] la même valeur juridique que celle des traités de l'Union. Elle est donc désormais contraignante pour les États membres et tout citoyen peut s'en prévaloir en cas de non-respect de ses droits. Elle repose sur le principe de la démocratie et le principe de l'État de droit.

En France et au sein de l'UE, les États étant des démocraties partageant les valeurs de la Déclaration universelle des droits de l'homme, de la Convention européenne des droits de l'homme et ayant donné une valeur supérieure à la Charte des droits fondamentaux, la conception, le développement et le déploiement des technologies de reconnaissance faciale doivent donc être juridiquement analysés dans ce cadre normatif.

LES DROITS FONDAMENTAUX SUSCEPTIBLES D'ÊTRE IMPACTÉS PAR L'UTILISATION DES TECHNOLOGIES DE RECONNAISSANCE FACIALE

Les technologies de reconnaissance faciale interrogent de nombreux droits fondamentaux consacrés par les textes susmentionnés.

L'Agence des droits fondamentaux de l'Union européenne (FRA) en a réalisé un examen précis dans le cadre de l'utilisation des technologies de reconnaissance faciale par les pouvoirs publics dans une note publiée au mois de novembre 2019[68]. Sont ainsi visés par cette Agence :

- la dignité humaine ;
- le respect de la vie privée ;

62 Organisation des Nations Unies (1948), Déclaration universelle des droits de l'homme : https://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/frn.pdf
63 Organisation des Nations Unies (1966), Pacte international relatif aux droits civils et politiques : https://www.ohchr.org/fr/professionalinterest/pages/ccpr.aspx
64 Organisation des Nations Unies (1966), Pacte international relatif aux droits économiques, sociaux et culturels : https://www.ohchr.org/FR/ProfessionalInterest/Pages/CESCR.aspx
65 Organisation des Nations Unies (1989), Convention relative aux droits de l'enfant : https://www.ohchr.org/fr/professionalinterest/pages/crc.aspx

66 Conseil de l'Europe (1950), Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales : https://www.echr.coe.int/Documents/Convention_FRA.pdf
67 Union européenne (2000), Charte des droits fondamentaux de l'Union européenne : https://www.europarl.europa.eu/charter/pdf/text_fr.pdf
68 Agence des droits fondamentaux de l'Union européenne (2019), « Facial recognition technology: fundamental rights considerations in the context of law enforcement », 36 pp. : https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law

- la protection des données à caractère personnel ;
- la non-discrimination ;
- les droits de l'enfant et des personnes âgées ;
- les droits des personnes handicapées ;
- la liberté de réunion et d'association ;
- la liberté d'expression ;
- le droit à une bonne administration ;
- le droit à un procès équitable.

TABLEAU 1 - EXEMPLES DE DROITS FONDAMENTAUX SUSCEPTIBLES D'ÊTRE IMPACTÉS PAR L'UTILISATION DES TECHNOLOGIES DE RECONNAISSANCE FACIALE

Droits ou libertés fondamentales[69]	Impact des technologies de reconnaissance faciale
Dignité humaine	Les technologies de reconnaissance faciale, notamment lorsqu'elles sont utilisées en direct, peuvent être perçues comme des technologies de surveillance tellement intrusives sur la vie des personnes qu'elles affectent leur capacité à mener une vie digne.
Non-discrimination	Une discrimination peut survenir lors de la conception (consciemment ou non) de l'algorithme lui-même (par l'introduction notamment de biais) ou résulter de l'application par les personnes qui décident des mesures à prendre selon le résultat de l'algorithme.
Libertés d'expression, d'association et de réunion	L'utilisation des technologies de reconnaissance faciale à travers des caméras vidéo installées dans l'espace public peut retenir les personnes de s'exprimer librement, les encourager à modifier leur comportement ou revenir à les présenter comme faisant partie d'un groupe d'individus. Certaines personnes pourraient ainsi renoncer à se réunir dans l'espace public par crainte des technologies de reconnaissance faciale. Cela peut également aller à l'encontre de la liberté de préserver son anonymat.
Le droit à un procès équitable	Ce droit repose tout d'abord sur l'information des personnes. Ainsi, toute absence de transparence pourrait être de nature à porter atteinte à ce droit[70]. Par ailleurs, les autorités publiques doivent mettre en place des procédures pour permettre aux personnes concernées d'élever des contestations et de porter des réclamations. Par exemple, les personnes doivent pouvoir s'opposer à ce qu'elles figurent dans une base de données de comparaison ou réclamer la réparation d'un dommage dû à une erreur d'interprétation des résultats de technologies de reconnaissance faciale.
Le droit à une bonne administration	Il renvoie à la notion d'explicabilité et repose sur un principe de transparence qui implique que les individus peuvent demander à connaître les raisons pour lesquelles une décision a été prise à leur encontre. En matière de technologies de reconnaissance faciale, il s'agirait pour l'administration ou la police de pouvoir expliquer à une personne les raisons pour lesquelles celle-ci a été arrêtée en fonction des résultats d'une technologie de reconnaissance faciale.
Droit à l'éducation	Un élève qui se verrait refuser l'accès à un établissement scolaire dans une région ayant rendu obligatoires les accès par le biais de technologies de reconnaissance faciale, et ne proposant aucune autre alternative d'accès pourrait invoquer son droit à l'éducation.

69 La distinction entre droit fondamental et liberté fondamentale tient au fait que la liberté est inhérente à la personne en tant qu'individu, alors que le droit est une obligation de l'État vis-à-vis des individus.

70 L'information des personnes est un préalable indispensable. À défaut d'une telle information, il n'est pas possible d'effectuer un recours. Voir par exemple : CJUE (21 décembre 2016), aff. C-203/15 & C-698/15, Tele2 Sverige AB v. Post- och telestyrelsen and Secretary of State for the Home Department v. Tom Watson and Others; CJUE (19 janvier 2010), aff. C-555/07, Seda Kücükdeveci v. Swedex GmbH & Co. KG.

Il n'est pas exclu que certains usages des technologies de reconnaissance faciale interrogent d'autres droits fondamentaux. Il est possible d'envisager par exemple l'interdiction de faire du corps humain et de ses parties, en tant que tels, une source de profit, dans le cas où la captation de visage par des technologies de reconnaissance faciale serait effectuée à des fins commerciales. Par ailleurs, ces droits ne sont pas exclusifs : un usage d'une technologie de reconnaissance faciale peut mettre en cause le respect d'une variété de droits fondamentaux.

En France, concernant la protection des données à caractère personnel et le respect de la vie privée, l'article 1er de la loi 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés prévoyait d'ailleurs déjà que « *l'informatique doit être au service de chaque citoyen. [...] Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques* ».

Comme l'indique l'Agence des droits fondamentaux de l'Union européenne, l'impact en termes de droits fondamentaux varie considérablement selon l'objet, le contexte et la portée de l'utilisation des technologies de reconnaissance faciale. Bien que certaines failles découlent du manque de précision de la technologie en elle-même, des impacts persistent même en cas d'absence totale d'erreur.

La plupart des droits fondamentaux précités sont non seulement consacrés par la Charte européenne des droits fondamentaux, mais également au niveau international. Cela signifie que le raisonnement relatif à la compatibilité des technologies de reconnaissance faciale avec les droits fondamentaux pourrait également trouver lieu à s'appliquer au-delà de l'UE.

Les principes reconnus au niveau international

Le principe de non-discrimination est internationalement reconnu : il est inscrit à l'article 2 de la Déclaration universelle des droits de l'homme. Plusieurs autres droits découlent du principe de non-discrimination afin de protéger des personnes vulnérables qui sont susceptibles de discrimination particulièrement forte. Une protection supplémentaire leur est accordée pour que l'égalité de dignité et de droit soit atteinte. Il en est ainsi pour les enfants, les personnes âgées et les personnes en situation de handicap. Le principe de non-discrimination raciale en est également issu.

Les droits à un recours effectif et à un procès équitable sont également consacrés par les articles 8 à 11 de la Déclaration universelle des droits de l'homme. Cela signifie en particulier qu'à partir du moment où une personne est arrêtée, il faut que la légitimité de l'arrestation soit démontrée.

La liberté d'expression est un droit crucial et reconnu comme un autre fondement de la démocratie. Elle est consacrée à l'article 19 de la Déclaration universelle des droits de l'homme et par l'article 19 du Pacte international relatif aux droits civils et politiques.

Les libertés de réunion et d'association sont une émanation de la liberté d'expression, mais sont consacrées en tant que telles au sein de la Déclaration universelle des droits de l'homme (article 20) et du Pacte relatif aux droits civils et politiques (articles 21 et 22).

COMMENT CONCILIER TECHNOLOGIES DE RECONNAISSANCE FACIALE ET RESPECT DES DROITS FONDAMENTAUX ?

La question qui se pose alors est celle de la conciliation de ces droits et principes fondamentaux avec les technologies de reconnaissance faciale. Le fait que les technologies de reconnaissance faciale soient susceptibles d'y porter atteinte doit appeler à la plus grande prudence.

Il en est ainsi de la dignité humaine qui est un droit « inviolable » comme l'indique l'article 1er de la Charte européenne des droits fondamentaux, ce qui signifie qu'aucune atteinte ne peut y être portée. Bien avant l'adoption de la Charte des droits fondamentaux de l'Union européenne, le Conseil d'État français avait dans son célèbre arrêt « Commune de Morsang-sur-Orge » du 27 octobre 1995 consacré le principe de respect de la dignité humaine comme composante de l'ordre public (affaire dite du « lancer de nain ») ; ce principe prévalant en l'espèce sur le consentement même de la personne. De même, le Conseil constitutionnel a également considéré que la sauvegarde de la dignité de la personne humaine constitue un principe à valeur constitutionnelle et la Cour de justice de l'Union européenne (CJUE) l'a reconnue comme principe général du droit[71]. De ce fait, si un dispositif de reconnaissance faciale porte atteinte à la dignité humaine, alors il doit être banni et aucune dérogation à cette règle n'est possible.

Alors que c'est exclu pour la dignité de la personne humaine (à laquelle aucune atteinte ne peut être portée), il est possible de limiter l'exercice des autres droits consacrés par la Charte des droits fondamentaux de l'UE, mais uniquement sous réserve de respecter certaines conditions. En effet, l'article 52 de la Charte des droits fondamentaux de l'Union européenne prévoit que « *toute limitation de l'exercice des droits et libertés reconnus par la présente Charte doit être prévue par la loi et respecter le contenu essentiel desdits droits et libertés. Dans le respect du principe de proportionnalité, des limitations ne peuvent être apportées que si elles sont nécessaires et répondent effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et libertés d'autrui.* »

Il s'ensuit que toute limitation portée aux droits consacrés par la Charte des droits fondamentaux de l'Union européenne doit :

- être prévue par la loi : c'est-à-dire relever d'un texte en vigueur ayant valeur juridique ;
- répondre véritablement à des objectifs d'intérêt général reconnus par l'Union ou à la nécessité de protéger les droits et libertés d'autrui ;
- respecter l'essence des droits et libertés, c'est-à-dire le noyau inaliénable du droit concerné ;

71 Conseil constitutionnel (27 juillet 1994), n° 94-343-344 DC ; CJUE (14 octobre 2004), Omega, aff C-36/02.

- respecter le principe de proportionnalité ;
- être nécessaire (principe de nécessité).

Si la mise en place d'une technologie de reconnaissance faciale est susceptible de porter atteinte à un droit fondamental et que cette limitation ne répond pas à l'une de ces conditions, son déploiement est susceptible d'être jugé contraire à la Charte des droits fondamentaux de l'Union européenne. Il est intéressant de noter à ce titre l'avis rendu par la CNIL sur le projet de décret afférent à l'application « StopCovid », dans lequel elle rappelle l'importance du respect des conditions susmentionnées, notamment le motif d'intérêt général et le principe de proportionnalité[72].

Sans avoir une portée aussi générale que le mécanisme prévu par la Charte des droits fondamentaux de l'Union européenne, la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales prévoit également un mécanisme similaire qui s'applique aux ingérences des autorités publiques dans l'exercice de certains droits consacrés par cette Convention, à savoir le droit au respect de la vie privée et familiale, la liberté de pensée, de conscience et de religion, la liberté d'expression, la liberté de réunion et d'association et la liberté de circulation. Les ingérences des autorités publiques doivent donc poursuivre certains buts définis par la convention et il doit s'agir de *« mesures nécessaires, dans une société démocratique »*[73] et proportionnées au but poursuivi.

Le principe de proportionnalité est un concept essentiel. Il se définit comme un *« mécanisme de pondération entre des principes juridiques de rang équivalent, simultanément applicables mais antinomiques*[74] *»*. Il s'agit d'opérer une mise en balance et de réaliser un équilibre entre chacun des principes juridiques en cause – généralement un pouvoir reconnu à l'État (ordre pu-

72 Délibération n° 2020-056 du 25 mai 2020 portant avis sur un projet de décret relatif à l'application mobile dénommée « StopCovid », §5 : *« La Commission rappelle néanmoins que les protections constitutionnelle et conventionnelle du droit au respect de la vie privée et à la protection des données à caractère personnel, assises notamment sur la Charte des droits fondamentaux de l'Union européenne et la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, imposent que les atteintes portées à ces droits par les autorités publiques soient non seulement justifiées par un motif d'intérêt général, comme cela est le cas en l'espèce, mais soient également nécessaires et proportionnées à la réalisation de cet objectif. »*

73 Conseil de l'Europe (1950), *op. cit.*

74 G. Xynopoulos, « Proportionnalité », in D. Alland et S. Rials (2003), *Dictionnaire de la culture juridique*, PUF, 2003, p. 1251.

blic, force publique) et des droits fondamentaux des personnes – ou entre plusieurs droits fondamentaux. Le respect du principe de proportionnalité impose qu'une mesure restreignant les droits et libertés soit à la fois :

- appropriée, en ce qu'elle doit permettre de réaliser l'objectif légitime poursuivi ;
- nécessaire, c'est-à-dire qu'elle ne doit pas excéder ce qu'exige la réalisation de cet objectif ;
- et proportionnée, en ce qu'elle ne doit pas, par les charges qu'elle crée, être hors de proportion avec le résultat recherché.

Si le principe de proportionnalité a d'abord été un mécanisme utilisé par les juges afin d'arbitrer entre des principes juridiques concurrents, ce triple test s'est vu conféré une portée générale au niveau européen. Il ressort en effet de l'article 5 du Traité sur l'Union européenne qu' « *en vertu du principe de proportionnalité, le contenu et la forme de l'action de l'Union n'excèdent pas ce qui est nécessaire pour atteindre les objectifs des traités. Les institutions de l'Union appliquent le principe de proportionnalité conformément au protocole sur l'application des principes de subsidiarité et de proportionnalité* ». Le principe de proportionnalité vise à limiter et à encadrer les actions de l'Union européenne qui doit s'en tenir à ce qui est nécessaire à la concrétisation des objectifs des traités. Cela implique en particulier que le législateur européen doit y avoir recours lorsqu'il adopte un texte.

D'origine allemande, le recours au triple test s'est progressivement développé en Europe[75], y compris au Royaume-Uni. Une certaine application du triple test commence également à se diffuser aux États-Unis[76]. En France, le Conseil constitutionnel utilise le contrôle de proportionnalité lorsqu'il contrôle des dispositions législatives qui restreignent l'exercice d'un droit ou d'une liberté

75 CEDH (23 juillet 1968), aff. n° 1474/62, Affaire «relative à certains aspects du régime linguistique de l'enseignement en Belgique c. Belgique» pts. 5 et 10 ; CEDH (4 décembre 2008), aff. 30562/04 & 30566/04 S. and Marper v. the United Kingdom, paras. 95-104 ; CJCE (24 juillet 2003), aff. C-280/00 Altmark ; CJUE (8 avril 2014), aff. C-293/12 & C-594/12, Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others.
76 Cour d'appel des États-Unis, 9ème district (9 février 2017), State of Washington c. Donald J. Trump et al., n° 17-35105. Dans cette décision, la Cour d'appel procède à une mise en balance des atteintes portées par le décret à certains droits individuels et des États avec l'intérêt général à le maintenir en vigueur.

au nom de la sauvegarde de l'ordre public ou lorsqu'il doit concilier plusieurs droits fondamentaux entre eux[77]. La Commission nationale de l'informatique et des libertés (CNIL) a régulièrement recours au contrôle de proportionnalité et de nécessité afin de vérifier la licéité d'un traitement. C'est précisément ce qu'elle a fait dans sa publication sur la reconnaissance faciale du 15 novembre 2019[78] ou lorsqu'elle s'est prononcée sur l'application visant à localiser les individus porteurs du Covid-19[79].

Le plein respect des droits fondamentaux est une condition préalable à toute application de la loi, quelles que soient les technologies en question. Il est donc nécessaire de mettre en œuvre le triple test avant tout déploiement des technologies de reconnaissance faciale. En outre, plus les technologies sont intrusives, plus le test doit être appliqué strictement.

LES RÉGLEMENTATIONS NATIONALES ET RÉGIONALES COMPLÈTENT LE CADRE ESQUISSÉ PAR LES DROITS FONDAMENTAUX

Au-delà des droits fondamentaux, qui se trouvent au sommet de la hiérarchie des normes, le déploiement des technologies de reconnaissance faciale doit également respecter diverses réglementations nationales qui pourraient trouver lieu à s'appliquer. Afin de nourrir le débat au niveau national et européen, il convient, au-delà du cadre normatif français et de l'UE, d'observer aussi les développements en cours à l'étranger, notamment aux États-Unis et en Chine. Cette dimension globale est d'autant plus importante que ces deux pays tentent d'imposer leurs standards dans le marché mondial des technologies de reconnaissance faciale[80].

77 Conseil constitutionnel (23 juillet 2015), n° 2015-713 DC, § 11 ; Conseil constitutionnel (22 décembre 2015), n° 2015-527 QPC, § 4 ; Conseil constitutionnel (10 février 2017), n° 2016-611 QPC.
78 « Reconnaissance faciale : pour un débat à la hauteur des enjeux », CNIL, 15 novembre 2019 : https://www.cnil.fr/fr/reconnaissance-faciale-pour-un-debat-la-hauteur-des-enjeux
79 Audition devant la commission des lois à l'Assemblée nationale, propos liminaires de Marie-Laure Denis, Présidente de la CNIL, mercredi 8 avril 2020 : « *Si un dispositif de suivi des personnes était mis en place de manière obligatoire, alors il nécessiterait une disposition législative et devrait, en tout état de cause, démontrer sa nécessité pour répondre à la crise sanitaire ainsi que sa proportionnalité en tenant compte des mêmes principes de protection de la vie privée, et en étant réellement provisoire* ».
80 « How the US plans to crack down on Chinese facial recognition tech used to 'strengthen authoritarian governments' », *This Week in Asia*, 18 juin 2019.

Avant d'examiner ces réglementations, il est intéressant de relever que ces technologies font l'objet de définitions juridiques depuis quelques temps déjà :

- selon le « Groupe de l'article 29 » (devenu aujourd'hui le Comité européen de la protection des données ou « EDPB »), « *la reconnaissance faciale est le traitement automatique d'images numériques qui contiennent le visage de personnes à des fins d'identification, d'authentification/de vérification ou de catégorisation de ces personnes* »[81] ;

- selon la Commission nationale de l'informatique et des libertés, « *la reconnaissance faciale est une technique informatique et probabiliste qui permet de reconnaître automatiquement une personne sur la base de son visage, pour l'authentifier ou l'identifier* »[82].

LE CADRE EN FRANCE

En France, les technologies de reconnaissance faciale ne sont pas encadrées par un texte spécifique. Elles sont toutefois soumises à la réglementation applicable aux traitements de données à caractère personnel et, dans une certaine mesure, à celle applicable à l'installation des dispositifs de vidéoprotection. Notons également que selon les usages, le recours à des technologies de reconnaissance faciale peut questionner d'autres droits que le droit à la protection des données personnelles ou au respect de la vie privée. C'est le cas du droit du travail, lorsque par exemple ces technologies sont utilisées pour un accès sécurisé à des locaux professionnels.

81 Avis 02/2012 sur la reconnaissance faciale dans le cadre des services en ligne et mobiles, 22 mars 2012.
82 «Reconnaissance faciale pour un débat à la hauteur des enjeux», CNIL, 15 novembre 2019.

La réglementation applicable aux données à caractère personnel

Une donnée à caractère personnel est toute information se rapportant à une personne physique identifiée ou identifiable[83]. Il existe des catégories particulières de données personnelles, dites « sensibles », dont les données biométriques[84]. Ces données sont soumises à un régime juridique plus strict que les autres.

Les technologies de reconnaissance faciale impliquant des données biométriques, elles sont à ce titre soumises à la réglementation applicable aux traitements de données à caractère personnel, c'est-à-dire :

- au règlement (UE) 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (Règlement général sur la protection des données ou « RGPD ») ;

- à la directive (UE) 2016/680 du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données (« Directive Police-Justice ») ; et

- à la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée (« Loi Informatique et Libertés »).

En France, des textes autorisant le recours à des technologies de reconnaissance faciale dans le cadre de traitements de données à caractère personnel ont été adoptés depuis longtemps. Pas moins de cinq autorisent expressément le recours aux technologies de reconnaissance faciale, à savoir, le traitement des antécédents judiciaires (TAJ), le passage rapide aux frontières ex-

83 RGPD, article 4 §1 : « *'données à caractère personnel', toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée «personne concernée») ; est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale* ».
84 RGPD, article 4 §14.

térieures (PARAFE), l'authentification en ligne certifiée sur mobile (ALICEM) et deux utilisations temporaires à des fins expérimentales (dans plusieurs aérodromes et dans le cadre d'un « hackathon »). Par ailleurs, ces technologies étant généralement considérées comme « suspectes » en droit français, il existe plus d'une vingtaine de textes mettant en place des traitements comportant des images numérisées d'individus qui excluent expressément, voire même qui interdisent le recours aux technologies de reconnaissance faciale, comme s'il s'agissait d'un véritable « garde-fou ».

Le RGPD – qui s'applique non seulement en France, mais également au sein de l'ensemble des États membres de l'Union européenne – impose de respecter un certain nombre de principes qui s'appliquent à tous les traitements de données à caractère personnel, y compris aux données biométriques et donc *a fortiori* aux technologies de reconnaissance faciale. Il s'agit notamment du :

- principe de licéité : tout traitement de données doit se fonder sur l'une des « bases légales » visées par le RGPD pour pouvoir être mis en œuvre ;
- principe de traitement loyal et transparent : la personne concernée doit être informée de l'existence de l'opération de traitement et de ses finalités (cette obligation se trouve renforcée à l'égard des mineurs grâce à l'utilisation de termes adaptés et compréhensibles) ;
- principe de limitation des finalités : les données doivent être collectées pour des finalités déterminées, explicites et légitimes ;
- principe de minimisation des données : les données doivent être adéquates, pertinentes, et limitées à ce qui est nécessaire au regard des finalités ;
- principe d'exactitude : les données doivent être exactes et à jour.

Avant l'entrée en vigueur du RGPD[85], les données biométriques n'étaient pas considérées comme des « données sensibles », c'est-à-dire des données qui ne peuvent pas, en principe, faire l'objet d'un traitement. Les données biométriques relevaient essentiellement du régime de demande d'autorisation auprès de la CNIL. En France, les personnes souhaitant mettre en œuvre des traitements de données à caractère personnel impliquant des technologies de reconnaissance faciale devaient ainsi obtenir l'autorisation préalable de la CNIL. Ces demandes d'autorisation ont donné lieu à plusieurs délibérations de la part de l'autorité[86]. Le traitement des données biométriques (et donc le recours aux technologies de reconnaissance faciale) est, en principe, interdit[87]. Il existe cependant un certain nombre d'exceptions à ce principe d'interdiction. S'agissant des données biométriques, et donc *a fortiori* des technologies de reconnaissance faciale, plusieurs exceptions sont susceptibles de s'appliquer notamment :

- lorsque la personne concernée a donné son consentement explicite ;
- lorsque le traitement est nécessaire à la sauvegarde d'intérêts vitaux ;
- lorsque le traitement est nécessaire pour des motifs d'intérêt public importants ;
- lorsque le traitement est nécessaire à des fins de recherche scientifique (mais celle-ci est pour l'instant limitée à la recherche publique en France).

Lorsque la base légale de traitement est le consentement explicite de la personne concernée, celui-ci doit non seulement être libre, spécifique, éclairé et univoque, mais il n'est de plus valable que si la personne concernée est en mesure de refuser ou de retirer son consentement sans subir de préjudice. Il est donc nécessaire de prévoir une solution alternative pour la personne concernée qui refuserait de donner son consentement ou déciderait de le retirer ultérieurement. Le RGPD précise que lorsque le responsable du traitement est une autorité publique, il est improbable que le consentement ait été donné librement, dès lors qu'il existe souvent un déséquilibre manifeste des rapports de force entre le responsable du traitement et la personne concernée[88].

85 C'est-à-dire sous la Directive 95/46/CE du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

86 À notre connaissance, quatorze délibérations ont autorisé le recours à des technologies de reconnaissance faciale et cinq l'ont refusé.

87 RGPD, article 9.

88 RGPD, considérants 42 et 43 ; Groupe de travail « Article 29 » lignes directrices sur le consentement au sens du règlement 2016/679.

Consentement préalable et proportionnalité : l'exemple du « contrôle d'accès virtuel » dans des lycées de la région PACA

Le tribunal administratif de Marseille a rendu le 27 février 2020 la première décision jurisprudentielle concernant la reconnaissance faciale en France. Le conseil régional de Provence-Alpes-Côte d'Azur (PACA) avait engagé l'expérimentation d'un dispositif dit « de contrôle d'accès virtuel » dans deux lycées, consistant en l'installation de portiques de reconnaissance faciale à l'entrée de ces établissements. La Région PACA a entendu justifier légalement le traitement de données biométriques par le consentement préalable des lycéens concernés. Le tribunal administratif de Marseille a fait droit à la demande d'annulation de la décision, en relevant notamment qu' « *alors que le public visé se trouve dans une relation d'autorité à l'égard des responsables des établissements publics d'enseignement concernés, la Région ne justifie pas avoir prévu des garanties suffisantes afin d'obtenir des lycéens ou de leurs représentants légaux qu'ils donnent leur consentement à la collecte de leurs données personnelles de manière libre et éclairée* ».

La CNIL avait par ailleurs été saisie par la Région Provence-Alpes-Côte d'Azur d'une demande de conseil portant sur cette expérimentation, qui avait préalablement fait l'objet d'une analyse d'impact relative à la protection des données, dont les résultats lui avaient été communiqués. Suivant délibération du 17 octobre 2019, la CNIL a relevé que les dispositifs de reconnaissance faciale étaient particulièrement intrusifs et présentaient des risques majeurs d'atteinte à la vie privée et aux libertés individuelles, notamment lorsqu'ils sont appliqués à des mineurs. En présence de moyens alternatifs moins intrusifs (par exemple, un contrôle par badge), l'autorité a considéré que le dispositif envisagé était contraire aux grands principes de proportionnalité et de minimisation des données posés par le RGPD.

Le RGPD prévoit par ailleurs la nécessité d'effectuer une analyse d'impact relative à la protection des données (AIPD) concernant les traitements de données à caractère personnel qui sont susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes concernées. Le recours aux technologies de reconnaissance faciale devrait nécessiter la mise en œuvre d'une AIPD, soit parce qu'elles constituent une opération définie par la CNIL pour laquelle une AIPD est obligatoire, soit parce qu'elles répondent à l'un ou plusieurs des critères issus des lignes directrices du « Groupe de l'article 29 »[89]. Parmi ces critères, le Groupe vise d'ailleurs expressément les technologies de reconnaissance faciale en évoquant le critère de l'utilisation innovante ou de l'application de nouvelles solutions technologiques ou organisationnelles[90]. S'il apparaît que le niveau de risque résiduel reste élevé, les résultats de l'AIPD doivent être communiqués à la CNIL.

A l'instar du RGPD, la Directive Police-Justice s'applique non seulement en France, mais également au sein de l'ensemble des États membres de l'Union européenne. Si les technologies de reconnaissance faciale sont utilisées à des fins de sécurité ou de prévention, celles-ci relèvent non pas du RGPD mais de la Directive Police-Justice. Cette directive constitue la « sœur jumelle » du RGPD et a été adoptée en même temps que ce dernier. Elle s'applique essentiellement aux traitements de données à caractère personnel effectués à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites ou d'exécution de sanctions pénales, y compris la protection et la prévention contre les menaces pour la sécurité publique.

Dans le cadre de la Directive Police-Justice, le traitement des données biométriques est autorisé dans les conditions prévues à l'article 10 : « *Le traitement des données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, ou l'appartenance syndicale, et le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de ma-*

89 Par exemple, la surveillance systématique, la collecte de données sensibles ou données à caractère hautement personnel, la collecte de données personnelles à large échelle, le croisement de données, les données concernant des personnes vulnérables (patients, personnes âgées, enfants, etc.) ou l'usage innovant (utilisation d'une nouvelle technologie).

90 Groupe de travail « Article 29 » sur la protection des données (2017), « Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est «susceptible d'engendrer un risque élevé» aux fins du règlement (UE) 2016/679 », p. 12 : « *Utilisation innovante ou application de nouvelles solutions technologiques ou organisationnelles : utilisation combinée, par exemple, de systèmes de reconnaissance des empreintes digitales et de reconnaissance faciale pour améliorer le contrôle des accès physiques, etc.* ».

nière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique est autorisé uniquement en cas de nécessité absolue, sous réserve de garanties appropriées pour les droits et libertés de la personne concernée, et uniquement :

a) lorsqu'ils sont autorisés par le droit de l'Union ou le droit d'un État membre ;

b) pour protéger les intérêts vitaux de la personne concernée ou d'une autre personne physique ; ou

c) lorsque le traitement porte sur des données manifestement rendues publiques par la personne concernée ».

Deux conditions sont donc exigées *a minima* par la Directive Police-Justice pour le traitement de données biométriques : il est possible de traiter des données biométriques (1) uniquement en cas de nécessité absolue, sous réserve de garanties pour les droits et libertés des personnes concernées et (2) uniquement lorsque ce traitement est autorisé par le droit de l'Union ou le droit d'un État membre.

La notion de « nécessité absolue » interroge puisque si une autre voie était possible – ce qui semble toujours être le cas[91] – cela pourrait revenir à exclure totalement la possibilité de recourir aux données biométriques et donc aux technologies de reconnaissance faciale. Il est difficile de répondre à cette question pour l'instant, car celle-ci n'a – à notre connaissance – pas été tranchée par la jurisprudence. La CNIL, lorsqu'elle est saisie pour avis, n'opère pas de contrôle à proprement parler sur cette notion, mais se concentre le plus souvent sur la mise en œuvre de garanties appropriées[92].

S'agissant du consentement des personnes, celui-ci ne peut constituer une base légale pour le traitement de données impliquant des technologies de reconnaissance faciale en vertu de la Directive Police-Justice. La mise en œuvre d'un dispositif à des fins sécuritaires nécessite *a minima* l'adoption d'une loi ou d'un décret en Conseil d'État. Toutefois, s'il s'agit d'une simple

91 Par exemple, s'agissant de l'utilisation de la reconnaissance faciale par les forces de police, il est toujours possible de recourir à du travail humain en procédant notamment à des filatures plutôt que de surveiller une masse d'individus à l'aide de caméras installées sur l'espace public.
92 Voir par exemple : Délibération n° 2019-123 du 3 octobre 2019 portant avis sur un projet de décret portant création d'un traitement automatisé de données à caractère personnel dénommé « application mobile de prise de notes » (GendNotes).

expérimentation, c'est-à-dire sans aller au-delà du test, cela relève du RGPD et, en définitive, il sera le plus souvent nécessaire d'obtenir le consentement des personnes volontaires.

Expérimentation du Carnaval de Nice 2019 : un rapport lacunaire selon la CNIL

Un dispositif de surveillance basé sur les technologies de reconnaissance faciale a été testé durant plusieurs jours dans la ville de Nice à l'occasion du carnaval en mars 2019. Près de 1 000 personnes ont accepté d'être identifiées au sein de la foule en temps réel par des technologies de reconnaissance faciale reposant sur six caméras positionnées dans le périmètre de test. La Ville de Nice a soulevé des difficultés juridiques qui ont entravé l'expérimentation et fait part de son souhait de voir évoluer la législation française en matière d'expérimentation de nouvelles technologies en conditions réelles sur la voie publique (et plus spécifiquement la Loi Informatique et Libertés). La CNIL a demandé des informations complémentaires notamment sur les taux d'erreurs des algorithmes, la qualité des images et les risques de discriminations, et a jugé le rapport de la Ville de Nice lacunaire.

La Loi Informatique et Libertés (LIL) est naturellement conforme à la logique prévue au sein des textes européens. L'article 6 de la Loi Informatique et Libertés renvoie d'ailleurs aux exceptions prévues par le RGPD concernant le traitement des données biométriques[93]. En l'occurrence, le RGPD permet le traitement de données biométriques dans certains cas bien précis, par exemple à des fins de recherche scientifique, lorsque cela est rendu nécessaire *« sur la base du droit de l'Union ou du droit d'un État membre »*[94]. Les États membres de l'UE disposent donc d'une certaine flexibilité, puisqu'ils peuvent permettre le traitement de données biométriques à des fins de recherche scientifique pour peu qu'ils adoptent des textes spécifiques. À l'heure actuelle, le législateur français et le pouvoir réglementaire n'ont ce-

93 Loi Informatique et Libertés, article 6.II : *« Les exceptions à l'interdiction mentionnée au I sont fixées dans les conditions prévues par le 2 de l'article 9 du règlement (UE) 2016/679 du 27 avril 2016 et par la présente loi »*.
94 RGPD, article 9 §2 (j).

pendant pas adopté de tels textes. Il n'est donc pas possible pour l'instant de traiter des données biométriques à des fins de recherche scientifique en France, hormis à des fins de recherche publique puisqu'un tel traitement est rendu possible par la Loi Informatique et Libertés[95].

Si un texte est nécessaire, les traitements mis en œuvre pour le compte de l'État impliquant des technologies de reconnaissance faciale devraient également donner lieu à un avis motivé de la CNIL et un décret en Conseil d'État[96].

La réglementation relative à la vidéoprotection

En France, en plus de la réglementation applicable aux données à caractère personnel (RGPD, Directive Police-Justice, Loi Informatique et Liberté), l'utilisation des technologies de reconnaissance faciale est encadrée par la réglementation relative à la vidéoprotection. Cette réglementation résulte essentiellement des articles L.251-1 et suivants du Code de la sécurité intérieure (CSI). Elle s'applique à l'installation de dispositifs de captation sur la voie publique et dans les lieux ouverts au public, à l'exclusion de ceux qui sont installés dans des lieux privés et lieux de travail non ouverts au public (« vidéosurveillance »). Au titre de cette réglementation, l'installation d'un dispositif de vidéoprotection nécessite de répondre à certaines finalités déterminées par le législateur[97], à savoir :

- la protection des bâtiments publics et installations publiques et de leurs abords ;
- la sauvegarde des installations utiles à la défense nationale ;
- la régulation des flux de transport ;

95 LIL, article 44 : *« L'article 6 ne s'applique pas si l'une des conditions prévues au 2 de l'article 9 du règlement (UE) 2016/679 du 27 avril 2016 est remplie, ainsi que pour [...] 6° Les traitements nécessaires à la recherche publique au sens de l'article L. 112-1 du code de la recherche, sous réserve que des motifs d'intérêt public important les rendent nécessaires, dans les conditions prévues par le g du 2 de l'article 9 du règlement (UE) 2016/679 du 27 avril 2016, après avis motivé et publié de la Commission nationale de l'informatique et des libertés rendu selon les modalités prévues à l'article 34 de la présente loi. »*

96 LIL, article 32 : *« Sont autorisés par décret en Conseil d'État, pris après avis motivé et publié de la Commission nationale de l'informatique et des libertés, les traitements de données à caractère personnel mis en œuvre pour le compte de l'État, agissant dans l'exercice de ses prérogatives de puissance publique, qui portent sur des données génétiques ou sur des données biométriques nécessaires à l'authentification ou au contrôle de l'identité des personnes. »*

97 CSI, article L. 251-2.

- la constatation des infractions aux règles de la circulation ;
- la prévention des atteintes à la sécurité des personnes et des biens dans des lieux particulièrement exposés à des risques d'agression, de vol ou de trafic de stupéfiants, ainsi que la prévention, dans des zones particulièrement exposées à ces infractions, des fraudes douanières ;
- la prévention d'actes de terrorisme ;
- la prévention des risques naturels ou technologiques ;
- le secours aux personnes et la défense contre l'incendie ;
- la sécurité des installations accueillant du public dans les parcs d'attraction ;
- le respect de l'obligation d'être couvert, pour faire circuler un véhicule terrestre à moteur, par une assurance garantissant la responsabilité civile.

Selon les finalités poursuivies, l'installation des systèmes de vidéoprotection relèvent également du RGPD, de la Directive Police-Justice ou de la Loi Informatique et Libertés[98].

Par ailleurs, la réglementation relative à la vidéoprotection impose également :

- d'informer les personnes susceptibles d'être filmées par voie d'affiches ou de panonceaux (l'obligation d'information résulte également du RGPD et de la Directive Police-Justice) ;
- de limiter la durée de conservation des enregistrements, qui ne peuvent être conservés au-delà d'un mois[99] ;
- d'assurer la sécurité des données traitées (par exemple en limitant le visionnage des images à des personnes habilitées).

98 Pour plus d'informations voir : « Vidéoprotection : quelles sont les dispositions applicables ? », CNIL, 13 décembre 2019 : https://www.cnil.fr/fr/videoprotection-quelles-sont-les-dispositions-applicables

99 CSI, article L.252-5.

L'installation d'un dispositif de vidéoprotection sur la voie publique doit en principe être autorisée par le préfet territorialement compétent, après avis de la Commission départementale de vidéoprotection. En revanche, si les systèmes installés sont utilisés dans le cadre de traitements de données à caractère personnel, leur installation doit être autorisée dans les conditions fixées par la réglementation applicable aux traitements de données à caractère personnel[100]. Il s'ensuit donc que l'installation de dispositifs de vidéoprotection intégrant *ab initio* des technologies de reconnaissance faciale est soumise aux dispositions de la réglementation relative aux traitements de données à caractère personnel. Toutefois, si des dispositifs de vidéoprotection sont installés et qu'à la suite de cette installation, des technologies de reconnaissance faciale sont utilisées à partir des enregistrements, il sera nécessaire de se conformer aux deux référentiels.

Des associations dénoncent un dispositif alliant vidéoprotection et reconnaissance faciale à Marseille

Deux associations, La Quadrature du Net et la Ligue des droits de l'Homme (LDH), ont déposé le 17 janvier 2020 un recours devant le tribunal administratif de Marseille, pour faire annuler le déploiement de technologies de reconnaissance faciale reposant sur un réseau d'une cinquantaine de caméras de vidéoprotection. Les requérants reprochaient notamment à la Ville de Marseille d'avoir mis en œuvre ce dispositif sans étude d'impact préalable, ni consultation de la Commission nationale de l'informatique et des libertés et sans établir la nécessité absolue de recourir à une telle technologie. Ce recours a toutefois été rejeté le 11 mars 2020 à défaut d'éléments permettant d'établir l'existence de la décision attaquée.

LE CADRE À L'ÉTRANGER

À l'instar de la France, aucun pays étranger n'a pour l'instant fait le choix d'adopter une réglementation spécifique concernant les technologies de reconnaissance faciale. Il n'en demeure pas moins que leurs usages tendent à se multiplier à l'échelle globale, et ce dans des cadres réglementaires variés. Bien qu'il soit difficile d'établir une cartographie des initiatives juridiques entreprises à l'étranger, certaines tendances se dessinent. Globalement, l'approche privilégiée chez nos voisins européens semble être celle de la prudence (régulation/expérimentation). À cet égard, le Royaume-Uni fait toutefois figure d'exception par son adoption relativement « décomplexée » des technologies de reconnaissance faciale, y compris à des fins sécuritaires dans l'espace public. En Chine, c'est plutôt l'approche de l'apprentissage par la pratique qui est privilégiée. Enfin, aux États-Unis, le cadre prend petit à petit la voie de la régulation, voire de l'interdiction dans certains états.

En Europe

Le Royaume-Uni est le seul pays en Europe à utiliser des technologies de reconnaissance faciale en public à partir de « vraies » bases de données, c'est-à-dire sans recourir à des tests comme ce fut le cas dans la ville de Nice. Outre-Manche, les technologies de reconnaissance faciale ont été déployées lors de plusieurs grands événements publics, notamment lors de concerts ou de matchs de rugby. Ce fut également le cas à l'occasion de la finale de la Ligue des champions de l'UEFA 2017 qui s'est tenue à Cardiff. Ce cas particulier a d'ailleurs donné lieu à la première arrestation grâce à un dispositif de reconnaissance faciale, d'un délinquant recherché pour violence domestique.

Le 4 septembre 2019, une première décision a été rendue par la Queen's Bench Divisional Court de la High Court of Justice siégeant à Cardiff. Les juges anglais ont considéré que l'utilisation des technologies de reconnaissance faciale était conforme à leur réglementation[101]. Un appel a été interjeté à l'encontre de cette décision.

100 CSI, article L252-1.

101 High Court of Justice, Queen's Bench Divisional Court, Cardiff, Case No: CO/4085/2018, R (Bridges) v CCSWP and SSHD : https://www.judiciary.uk/wp-content/uploads/2019/09/bridges-swp-judgment-Final03-09-19-1.pdf

L'ICO encourage la mise en place d'un code de pratique contraignant sur l'usage de la reconnaissance faciale par la police dans les lieux publics

Au mois d'août 2019, un promoteur immobilier a fait installer et a testé un système utilisant de la reconnaissance faciale dans le quartier très fréquenté de King's Cross à Londres. Le système installé au coin de l'un des bâtiments de la société filmait les passants dans la rue sans avertir ces derniers. La police a semble-t-il partagé des «*watchlists*» avec la société pour réaliser des opérations d'identification des personnes fichées. L'Information Commissioner's Office (ICO), équivalente de la CNIL au Royaume-Uni, enquête actuellement sur l'utilisation qui a été faite par la société de la reconnaissance faciale. À la suite de cette affaire, l'ICO a publié un rapport sur les usages des technologies de reconnaissance faciale par la police dans les lieux publics. L'Information Commissioner de l'ICO a également, dans un communiqué, demandé au gouvernement d'adopter un code de pratique contraignant sur le sujet, tout en rappelant à la police qu'elle devait ralentir et justifier des usages effectués.

En Allemagne, le législateur a fait usage de l'autorisation prévue à l'article 9 (2) (j) du RGPD prévoyant que le traitement de données sensibles est possible sans consentement à des fins de recherche scientifique lorsqu'il est nécessaire à cette finalité et que les intérêts du responsable du traitement l'emportent largement sur les intérêts de la personne concernée. En revanche, un projet de loi visant à actualiser le texte actuel qui réglemente les pouvoirs de la police a été purgé de ses références explicites à la reconnaissance faciale[102], le responsable fédéral pour la protection des données et l'ordre des avocats allemands ayant émis des doutes sur la compatibilité du projet avec la Constitution.

Aux Pays-Bas, le législateur a également fait usage de l'autorisation prévue à l'article 9 (2) (j) du RGPD à condition que le traitement soit nécessaire à des fins de recherche scientifique, que les recherches soient dans l'intérêt public, que la demande de consentement explicite s'avère impossible ou implique un effort disproportionné, et que l'exécution prévoie des garanties de façon à ce que la vie privée de la personne concernée ne soit pas affectée de manière disproportionnée.

102 Une version précédente du projet de loi envisageait d'autoriser la police fédérale à utiliser des technologies de reconnaissance faciale sur la base d'images collectées dans 135 gares ferroviaires et 14 aéroports.

En dehors de l'Europe

Aux États-Unis, la *Federal Trade Commission* (FTC) a publié dès le mois d'octobre 2012 des bonnes pratiques destinées aux sociétés souhaitant développer et commercialiser des technologies de reconnaissance faciale[103]. De nombreux états américains font un usage des technologies de reconnaissance faciale, tantôt pour le contrôle des fraudes (Texas[104], Washington[105] et Illinois[106] entre autres), tantôt pour la vérification d'identité (Montana[107], Nevada[108], Connecticut[109] ou encore Dakota du Nord[110]). Par ailleurs, l'année 2019 et le début de l'année 2020 ont été particulièrement riches en actualités s'agissant du recours aux technologies de reconnaissance faciale aux États-Unis :

- en mars 2019, le *Commercial Facial Recognition Privacy Act of 2019* a été présenté au Sénat. Ce texte prévoit l'obligation pour les entreprises privées de recevoir le consentement des personnes avant d'utiliser des technologies de reconnaissance faciale ;

103 « FTC Recommends Best Practices for Companies That Use Facial Recognition Technologies », FTC, 22 octobre 2012 : https://www.ftc.gov/news-events/press-releases/2012/10/ftc-recommends-best-practices-companies-use-facial-recognition

104 Texas Transportation Code, Titre 7, Sous-titre B, Chapitre 521, Sous-chapitre A : https://statutes.capitol.texas.gov/Docs/TN/htm/TN.521.htm

105 Washington State Legislature, RCWs, Titre 46, Chapitre 46.20, Section 46.20.037 : https://app.leg.wa.gov/RCW/default.aspx?cite=46.20.037

106 Illinois General Assembly, Illinois Compiled Statutes, Public Health (410 ILCS 705/) : http://www.ilga.gov/legislation/ilcs/ilcs4.asp?DocName=041007050HArt%2E+15&ActID=3992&ChapterID=35&SeqStart=3000000&SeqEnd=6400000

107 Montana Code annotated 2019, Title 1 'General Laws And Definitions', 'Chapter 5 'Proof And Acknowledgment Of Instruments Notaries Public', Part 6. Notarial Acts, 1-5-602. 'Definitions' : https://leg.mt.gov/bills/mca/title_0010/chapter_0050/part_0060/section_0020/0010-0050-0060-0020.html

108 Nevada Revised Statutes, Chapter 133 'Wills », NRS 133.085 : https://www.leg.state.nv.us/NRS/NRS-133.html#NRS133Sec085

109 General Statutes of Connecticut, Volume 6, Chapter 319o, Department of Social Services, Sec. 17b-30. 'Biometric identifier system' : https://www.cga.ct.gov/current/pub/chap_319o.htm#sec_17b-30

110 North Dakota Century Code, Chapter 44-04 'Duties, Records, and Meetings' : CHAPTER 44-04 : https://www.legis.nd.gov/cencode/t44c04.pdf

- en mai 2019, San Francisco est devenue la première Ville américaine à interdire son usage par la police et les services de la municipalité. D'autres Villes l'ont d'ailleurs imitée, notamment Oakland et Berkeley ;

- le 8 octobre 2019, la Californie a adopté le *Body Camera Accountability Act* (ou « AB 1215 ») interdisant l'utilisation de la reconnaissance faciale sur les caméras corporelles portées par les policiers ; dans la lignée, la Ville de San Diego, dont la police utilisait des technologies de reconnaissance faciale depuis 2012, a décidé de bannir leur utilisation pendant au moins trois ans, celles-ci n'ayant permis aucune arrestation ni poursuite ;

- en octobre 2019, dans l'état de New-York, une proposition obligeant les entreprises à informer les usagers de l'utilisation des technologies de reconnaissance faciale, de la durée de conservation des données et de leur transfert à des tiers a été présentée ;

- le 14 novembre 2019, un projet de loi a été présenté au Sénat. Les agents fédéraux doivent obtenir l'approbation d'un juge avant d'utiliser des technologies de reconnaissance faciale pour surveiller un criminel suspect[111] ;

- le 31 mars 2020, l'État de Washington a adopté une loi obligeant les agences gouvernementales à obtenir un mandat préalablement à toute utilisation de technologies de reconnaissance faciale, sauf en cas d'urgence[112]. Conformément à cette loi, le dispositif utilisé doit également pouvoir être testé de manière indépendante, afin de s'assurer qu'il ne cause pas de biais basés sur la couleur de la peau, le genre, l'âge et d'autres caractéristiques. La loi exige également, préalablement à tout déploiement par les autorités de l'État ou les collectivités locales, la rédaction de rapports de responsabilisation *(« accountability reports »)*[113] et la formation des agents.

111 Senate of the United States, 116th Congress, 1st Session, « Bill to limit the use of facial recognition technology by Federal agencies, and for other purposes » : https://www.coons.senate.gov/imo/media/doc/ALB19A70.pdf

112 « Washington State Signs Facial Recognition Curbs Into Law; Critics Want Ban », *U.S. News*, 31 mars 2020 : https://www.usnews.com/news/us/articles/2020-03-31/washington-state-adopts-facial-recognition-rules-critics-view-as-too-loose

113 « Washington State's regulation of facial recognition technology: first thoughts », *Global Partners Digital*, 24 avril 2020 : https://www.gp-digital.org/washington-states-regulation-of-facial-recognition-technology-first-thoughts/

Le FBI et l'Agence américaine de contrôle de l'immigration et des douanes dans la controverse

En juillet 2019, il a été révélé que le FBI et l'Agence de contrôle de l'immigration et des douanes (ICE) avaient scanné les visages de millions d'Américains sans leur consentement grâce aux bases de données des permis de conduire, et s'en étaient servis en lien avec des technologies de reconnaissance faciale. Cette utilisation n'a pourtant jamais été autorisée par le Congrès américain et les citoyens concernés n'ont jamais été informés de l'utilisation de leurs données personnelles et de leur photographie. Près de 390 000 recherches par reconnaissance faciale auraient ainsi été effectuées par le FBI depuis 2011.

En Chine, depuis plusieurs années, le modèle de gouvernance se construit sur la base de la collecte et du traitement massif des données personnelles des citoyens sur les réseaux sociaux et par le biais de caméras de surveillance. Un système de crédit social a même été mis en place dans certaines régions et permet aux autorités d'attribuer des scores aux citoyens en fonction de leurs comportements. Si leur score est trop bas, les individus sont sanctionnés par la privation de leurs droits les plus élémentaires (accès au crédit, circulation en train, accès aux écoles, etc.). En Chine, les données issues de la reconnaissance faciale constituent des « informations personnelles » aux termes de l'article 76 de la loi sur la cybersécurité[114]. Toutefois, il n'existe pas de cadre réglementaire unifié concernant la reconnaissance faciale, mais plutôt une multitude de règles spécifiques à certains secteurs :

- le 21 janvier 2020, la Payments & Clearing Association of China a publié une Convention d'autorégulation du secteur des paiements hors ligne par reconnaissance faciale ;

- une loi entrée en vigueur en décembre 2019 prévoit l'obligation pour les opérateurs de télécommunications mobiles d'enregistrer les données biométriques du visage de tout nouvel utilisateur cherchant à s'abonner à leurs services.

114 « Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017) », *New America*, 29 juin 2018 : https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/

En novembre 2019, une première plainte a été déposée dans le pays contre une entreprise ayant recours aux technologies de reconnaissance faciale. Détenteur d'un abonnement pour l'accès à un parc naturel, un professeur de droit a allégué une violation contractuelle contre le parc qui a changé la méthode d'identification à l'entrée.

De manière générale, la Chine adopte une approche d'apprentissage par la pratique en matière d'encadrement légal des technologies de reconnaissance faciale et leur usage n'est pas limité en amont par le législateur, mais au contraire borné par les possibilités techniques des industriels. Cependant, dans le cadre du renforcement du régime réglementaire de protection des informations personnelles, les autorités étatiques chargées de la supervision du marché chinois ont publié une nouvelle version des standards de protection des informations personnelles le 6 mars 2020[115]. Ces nouveaux standards imposent aux responsables de traitement d'informer les personnes concernées des règles de collecte, d'utilisation et de conservation des données issues des technologies de reconnaissance faciale et d'obtenir leur consentement pour le traitement de leurs données[116].

Il ressort de l'analyse du cadre juridique applicable aux technologies de reconnaissance faciale que le développement de ces dernières est relativement bien encadré juridiquement au sein de l'UE. Le RGPD, la Directive Police-Justice, ainsi que des législations nationales (par exemple la Loi Informatique et Libertés en France) ont été érigés pour protéger nos données personnelles, y compris nos données biométriques. Placés au sommet de la hiérarchie des normes, les droits fondamentaux constituent également des garde-fous censés nous protéger d'un déploiement des technologies de reconnaissance faciale susceptible de mettre à mal les principes de la démocratie et de l'État de droit. Afin de s'assurer que ce cadre remplit bien sa mission, il convient toutefois, au-delà de l'analyse théorique, de s'interroger sur son application. Un cadre juridique n'est en effet utile aux citoyens que s'il est effectivement (et aisément) applicable.

115 « China tightens protection of personal information - what you need to know about the 2020 Chinese Personal Information National Standard », *Lexology*, 23 maes 2020 : https://www.lexology.com/library/detail.aspx?g=5a63a595-4116-4567-bea2-f6b3380540cb

116 « China introduces stricter facial recognition standards », *South China Morning Post*, 10 mars 2020 : https://www.scmp.com/tech/article/3074443/china-introduces-stricter-facial-recognition-standards

UN CADRE JURIDIQUE QUI PÂTIT DE PROFONDES FAIBLESSES DANS SON APPLICATION

UNE APPLICATION FLUCTUANTE PARMI LES ÉTATS MEMBRES

Le RGPD et la Directive Police-Justice n'ont pas permis d'harmoniser complètement le cadre juridique applicable au traitement des données à caractère personnel au sein de l'Union européenne, en particulier en ce qui concerne le traitement des données biométriques. Certaines exceptions au principe de l'interdiction du traitement des données sensibles, dont font partie les données biométriques, nécessitent en effet pour leur mise en œuvre l'adoption d'un texte national ou européen. Pour l'instant, seuls quelques États ont décidé de franchir le pas, notamment en ce qui concerne l'exception à des fins de recherche scientifique. D'un État membre à l'autre, il peut donc exister des différences significatives dans l'application du cadre, en particulier dans le domaine de la recherche. Comme précédemment indiqué, en France, le traitement de données biométriques dans le cadre de la recherche n'est envisageable qu'à certaines conditions et seulement à des fins de recherche publique. À l'heure actuelle, aucune dérogation n'est prévue pour la recherche privée à proprement parler.

En outre, n'est pas non plus prévue pour l'instant l'adoption d'un texte européen qui permettrait certainement de niveler les disparités entre les États membres et d'harmoniser les règles de mise en œuvre, par exemple en ce qui concerne l'adoption d'un cadre méthodologique expérimental. Un projet de livre blanc sur l'intelligence artificielle émanant de la Commission européenne a fuité en janvier 2020, qui contenait une interdiction totale pendant plusieurs années d'utiliser des technologies de reconnaissance faciale dans les espaces publics européens afin de laisser le temps d'évaluer les impacts de ces technologies et de les réglementer. La version du livre blanc finalement pu-

bliée le 19 février 2020 ne reprend pas cette interdiction et ouvre au contraire la voie à une réflexion qui devrait être engagée à l'échelon européen[117].

Au surplus, il arrive même de constater des différences d'interprétation au sein d'un même État. C'est ce qui s'est produit au Royaume-Uni.

En France, des expérimentations sont menées par des acteurs privés et publics, le plus souvent avec les conseils de la CNIL. Les résultats de ces expérimentations ne sont cependant pas partagés entre les différents acteurs et les prestataires se livrent une bataille à distance afin de tenter d'imposer leur technologie. Il n'existe à l'heure actuelle pas de méthodologie d'expérimentation fiable et respectueuse des droits et libertés des citoyens. De même, l'amélioration de la performance des technologies de reconnaissance faciale nécessite d'accéder à des bases de plus en plus volumineuses d'images. À des fins de recherche fondamentale, il est donc peut-être opportun de permettre aux fournisseurs européens et français d'accéder à des bases de données dans des conditions respectueuses des droits et libertés des individus de manière à préserver leur compétitivité.

Enfin, les autorités de contrôle ne disposent pas toutes des mêmes moyens au sein de l'Union européenne. Globalement, leur efficacité se trouve en outre limitée par la faiblesse des budgets leur étant alloués par les États membres. À cet égard, un rapport paru récemment démontre notamment que le manque d'experts techniques représente un frein majeur à l'application du RGPD en Europe.[118] Le rapport souligne en effet que, parmi les 28 instances nationales chargées de l'application du RGPD, seules 5 comptent plus de 10 spécialistes techniques. De fait, les autorités chargées de la protection des données ne seraient souvent pas en mesure de défendre des actions en justice face aux multinationales, qui elles mobilisent des ressources financières considérables pour contester les injonctions des autorités devant les tribunaux. Il en résulte que les autorités chargées de faire appliquer le RGPD ne sont pas en capacité d'enquêter sur les plus grands acteurs du numérique. Il serait donc également utile de réfléchir à l'amélioration des moyens mis à leur disposition, afin notamment de leur permettre d'auditer les conditions liées au déploiement des technologies de reconnaissance faciale. Il est urgent de donner à ces autorités les moyens de vérifier si le recours à des technologies de reconnaissance faciale s'effectue ou non dans des conditions respectueuses de la réglementation.

117 Commission européenne (2020), « Intelligence artificielle : une approche européenne axée sur l'excellence et la confiance », p. 26 : « Afin de répondre aux éventuelles inquiétudes, du point de vue de la société, quant à l'utilisation de l'IA à de telles fins dans les lieux publics et d'éviter toute fragmentation du marché intérieur, la Commission lancera un vaste débat européen sur les circonstances particulières, le cas échéant, qui pourraient justifier une telle utilisation, ainsi que sur les garanties communes à mettre en place».

118 « Europe's governments are failing the GDPR - Brave's 2020 report on the enforcement capacity of data protection authorities », *Brave* : https://brave.com/wp-content/uploads/2020/04/Brave-2020-DPA-Report.pdf

DES DIFFICULTÉS D'APPLICATION QUI ENTRAÎNENT UN MANQUE D'EFFICIENCE

LES DIFFICULTÉS D'APPLICATION DES DROITS FONDAMENTAUX

Si les droits fondamentaux et l'application du triple test devraient s'imposer, force est de constater que le triple test est davantage utilisé par les juridictions en cas de contentieux que par le législateur. Il n'existe, en outre, pas de mécanisme qui permettrait de le rendre contraignant *a priori*.

L'application frileuse du triple test par le législateur et les autorités publiques

Si le triple test devrait s'imposer au législateur et aux autorités publiques, il faut reconnaître qu'il n'en est fait qu'un usage parcimonieux et rarement explicite. Il serait pourtant utile d'en avoir une démonstration systématique, notamment dans le cadre des évaluations préalables des projets de normes ou lors du processus d'adoption des décisions administratives.

Dans le cas des expérimentations de technologies de reconnaissance faciale qui ont été menées en France, il est fort probable que l'utilisation du triple test aurait été utile, ne serait-ce que pour valider leur déploiement, l'adapter ou l'interdire.

Actuellement, la protection des données à caractère personnel et de la vie privée concentrent l'essentiel des préoccupations lorsqu'un usage des technologies de reconnaissance faciale est envisagé, alors même que leur déploiement est susceptible de porter atteinte à d'autres droits fondamentaux. La généralisation du recours au triple test permettrait de faire une évaluation essentielle en termes de compatibilité des usages avec l'ensemble des droits et libertés fondamentales.

L'application ex post *du triple test par la jurisprudence*

S'agissant de la jurisprudence, celle-ci intervient généralement *ex post* et, le plus souvent, afin de sanctionner un usage ou un comportement. Les juges font usage du principe de proportionnalité et recourent au triple test depuis plusieurs décennies. Toutefois, pour que ceux-ci soient amenés à se prononcer et à faire application du triple test, encore faut-il qu'ils soient saisis d'un recours. La problématique rencontrée dans l'application des droits fondamentaux et du triple test est donc fortement tributaire de la contestation émanant des personnes concernées et de la saisine des juridictions compétentes.

Or, s'agissant des droits fondamentaux, les principaux textes applicables sont internationaux et européens. Les recours devant une instance internationale ou devant la Cour européenne des droits de l'homme – même si les juges nationaux peuvent également statuer sur cette question – sont particulièrement complexes et longs[119]. Pour atteindre la Cour de justice de l'Union européenne (CJUE), il faut préalablement qu'un recours ait été initié au niveau national et qu'une question préjudicielle soit posée, à moins qu'un recours en manquement ait été intenté par la Commission européenne à l'encontre d'un État membre. En tout état de cause, ces procédures sont particulièrement chronophages, ce qui provoque un décalage avec le déploiement des technologies mises en cause qui évoluent très rapidement. La décision sera ainsi rendue alors que la technologie de reconnaissance faciale aura été déployée ou sur le point de l'être :

- si la technologie est déjà déployée, il y aura potentiellement une atteinte aux droits fondamentaux et donc également un préjudice subi par les personnes concernées. Par définition, il ne sera plus possible de revenir en arrière pour les personnes dont les droits et libertés auront été bafoués. Se pose alors la question de la réparation des préjudices subis et des conséquences des éventuelles sanctions prononcées à l'encontre des États ;

- si la technologie est sur le point d'être déployée, il est possible de recourir à la procédure de référé-liberté sous réserve de respecter les trois conditions requises, à savoir l'urgence, l'atteinte à une liberté fondamentale et la démonstration que l'atteinte portée à cette liberté est grave et manifestement illégale[120].

Toutefois, cela exige que les personnes concernées saisissent les juridictions compétentes pour faire respecter leurs droits fondamentaux, ce qui suppose une surveillance constante et régulière des textes et projets potentiellement déployés par les autorités publiques. Il existe, certes, des associations de défense des droits qui s'attachent à cette mission, mais elles ne disposeront pas nécessairement des moyens pour agir, notamment si les technologies de reconnaissance faciale venaient à se multiplier. En France, La Quadrature du Net et la Ligue des droits de l'Homme introduisent régulièrement des recours à l'encontre des déploiements des technologies de reconnaissance faciale. Elles ont dernièrement fait annuler par le tribunal administratif de Marseille la décision par laquelle le conseil régional de Provence-Alpes-Côte d'Azur avait approuvé la mise en place d'un dispositif de contrôle d'accès par comparaison faciale et de suivi de trajectoire dans des lycées de la région.

En matière judiciaire, dans le cas d'un recours contre une entreprise privée déployant une technologie de reconnaissance faciale, les procédures sont également longues et complexes. Même si les référés sont possibles, plusieurs mois s'écoulent généralement avant l'obtention d'une décision.

En définitive, il est légitime se demander s'il est souhaitable de s'en remettre uniquement aux particuliers et aux associations de défense des droits pour faire respecter nos droits fondamentaux en cas de déploiement des technologies de reconnaissance faciale, étant données les contraintes inhérentes au contentieux administratif et judicaire.

L'absence de contraintes a priori

À ce jour, il n'existe aucun mécanisme de contrôle *a priori* ou d'obligation de réaliser une étude d'impact préalable au déploiement de technologies de reconnaissance faciale sur le fondement du respect des droits fondamentaux, en dehors de ceux imposés par la réglementation relative au traitement des données à caractère personnel. Alors qu'il existe une volonté de lancer plusieurs expérimentations et de les encadrer, il n'a pour l'instant jamais été question de mettre en œuvre cette analyse préalable au regard des droits fondamentaux. De nombreuses voix appellent pourtant à une réflexion en

119 Voir le schéma « Le cheminement d'une enquête » réalisé par la Cour européenne des droits de l'homme : https://www.echr.coe.int/Documents/Case_processing_FRA.pdf

120 Code de justice administrative, article L521-2.

profondeur sur le sujet des technologies de reconnaissance faciale, tant celles-ci ont le potentiel d'impacter le fondement même des démocraties. Il en est ainsi tant au niveau européen avec l'Agence des droits fondamentaux de l'UE (FRA) ou le Contrôleur européen de la protection des données, qu'au niveau national avec la CNIL ou à travers quelques initiatives menées par des parlementaires.

S'agissant de la réglementation relative au traitement des données à caractère personnel, il faut noter la disparition quasi généralisée du régime de l'autorisation préalable et la responsabilisation des acteurs procédant à des traitements de données à caractère personnel. Chaque responsable de traitement doit ainsi procéder à une évaluation des risques et, en particulier, réaliser sa propre analyse d'impact relative à la protection des données (AIPD). Toutefois, se pose la question de la soumission systématique des AIPD aux autorités de contrôle, par exemple à la CNIL en France.

La Commission européenne, dans son livre blanc dédié à l'intelligence artificielle, indique qu' « *il est capital que l'IA européenne soit fondée sur nos valeurs et nos droits fondamentaux, tels que la dignité humaine et la protection de la vie privée* » et envisage différents mécanismes de certification et labellisation permettant d'avoir un contrôle *a priori*[121].

LA QUESTION DE LA RESPONSABILITÉ

Outre les difficultés d'application des droits fondamentaux, la question de la responsabilité constitue une autre faiblesse inhérente au cadre juridique entourant les technologies de reconnaissance faciale. Ce problème épineux se pose de manière différente non seulement selon les pays, mais également selon le référentiel considéré (protection des données personnelles, de la vie privée, etc.).

Au regard de la réglementation relative au traitement des données à caractère personnel, c'est d'abord le responsable de traitement – c'est-à-dire la personne qui définit les moyens et la finalité du traitement – qui est responsable vis-à-vis des individus, même si les sous-traitants peuvent également voir leur responsabilité engagée depuis l'entrée en vigueur du RGPD.

121 Commission européenne (2020), « Intelligence Artificielle : une approche européenne axée sur l'excellence et la confiance », p. 2.

Au regard du droit de la responsabilité civile, la mise en œuvre de la responsabilité (contractuelle ou délictuelle) est subordonnée à la réunion de trois conditions cumulatives, à savoir une faute, un dommage et un lien de causalité entre les deux :

- la responsabilité contractuelle désigne l'obligation de réparer les dommages résultant d'un défaut dans l'exécution d'un contrat (inexécution, mauvaise exécution ou exécution tardive). Par exemple, si des technologies de reconnaissance faciale causent un dommage direct au client utilisateur, le fournisseur de ces technologies pourrait être tenu de le réparer ;

- la responsabilité délictuelle désigne l'obligation de réparer les dommages causés à autrui en dehors de tout lien contractuel. La question de la responsabilité des fournisseurs de technologies de reconnaissance faciale vis-à-vis des tiers se pose dans des termes substantiellement similaires à celle qui se pose pour l'intelligence artificielle. En droit français, la « responsabilité du fait des choses » repose essentiellement sur le contrôle de la chose au moment de la survenance du fait dommageable, ce qui n'est pas nécessairement adapté à l'intelligence artificielle. Il en est de même s'agissant de la réglementation relative à la sécurité des produits – qui impute la responsabilité au producteur du produit mis sur le marché –, notamment lorsque l'intelligence artificielle est incorporée après la mise sur le marché du produit par une partie qui n'est pas le producteur.

Quoi qu'il en soit, la question de la responsabilité concernant les technologies de reconnaissance faciale doit se poser pour l'ensemble des acteurs tout au long de la chaîne de responsabilité, qu'il s'agisse des concepteurs de l'algorithme, des fournisseurs de solutions, des acteurs privés et publics qui déploient ces technologies, ou des utilisateurs.

D'aucuns s'interrogent le plus souvent sur la responsabilité des fournisseurs, mais peut-être pas assez sur celle des utilisateurs. En effet, les technologies de reconnaissance faciale permettent d'obtenir un pourcentage de chances que le gabarit A corresponde au gabarit B et, à partir de ce résultat, un individu décide ensuite s'il est nécessaire ou non d'intervenir. Il est donc important que cet individu dispose des connaissances suffisantes pour prendre une décision, mais aussi et surtout pour aborder la personne concernée en

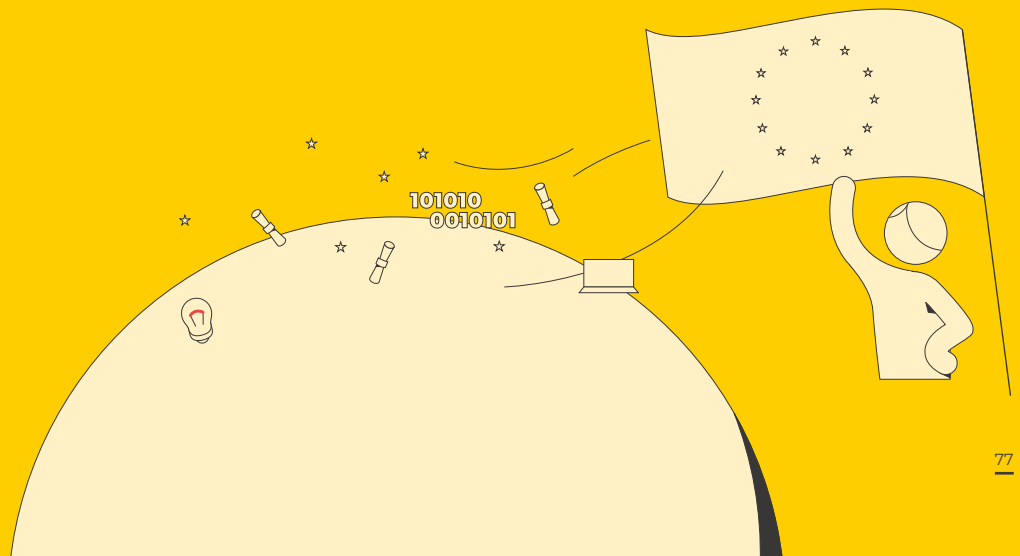
gardant à l'esprit qu'il s'agit seulement d'une correspondance potentielle et non forcément avérée (voir Section 1.3.3.).

Enfin, il ne faut pas non plus oublier la question de la responsabilité pénale, qui est également susceptible de se poser en particulier pour les clients utilisateurs, par exemple, au regard des sanctions pénales attachées au non-respect de la réglementation relative aux traitements de données à caractère personnel[122].

> *In fine*, force est de constater que, bien que le cadre juridique qui entoure le déploiement des technologies de reconnaissance faciale soit bien fourni, ce dernier pâtit de sérieuses faiblesses dans sa mise en œuvre. Il est notamment complexe d'assurer la conformité de ces technologies avec nos droits fondamentaux en l'absence de contrôle *a priori*. Quant aux analyses réalisées *ex post* par les juges, ces dernières demandent d'une part que le juge soit saisi, et d'autre part un investissement considérable de la part du requérant, notamment en termes de temps et de compétences. Tout un chacun n'en a tout simplement pas les moyens. Pour ce qui est de la seule protection de nos données personnelles, donc de nos données biométriques, ce sont le manque d'harmonisation au niveau européen, ainsi que le manque de moyens alloués aux autorités de contrôle, qui sont en cause. Si l'objectif est de garantir un déploiement des technologies de reconnaissance faciale conforme aux valeurs européennes, c'est-à-dire aux principes de l'État de droit et de la démocratie, alors nous ne pouvons nous satisfaire de cette situation. À l'heure où de plus en plus de technologies de reconnaissance faciale sont déployées, il est urgent que l'Union européenne se saisisse de ces enjeux et que les États membres s'accordent pour se doter d'un système robuste permettant de garantir nos droits.

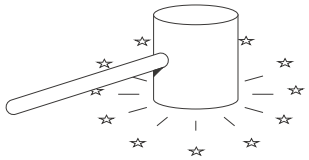
122 Code pénal, articles 226-16 et suivants.

PARTIE 3
VERS UN SYSTÈME DE STANDARDISATION EUROPÉEN GARANT DES DROITS ET LIBERTÉS FONDAMENTAUX



Le traitement de données biométriques sans contact confère aux dispositifs de reconnaissance faciale un caractère hautement sensible qui nécessite une vigilance renforcée de la société. Laisser la porte ouverte à la surveillance de masse n'est pas une option et la frontière entre les usages de ces technologies est souvent poreuse. Comment peut-on dès lors se protéger de la mise en péril de nos droits et libertés fondamentales ? Plusieurs pistes ont émergé dans le débat depuis plusieurs mois, allant de l'interdiction totale des technologies de reconnaissance faciale à l'amélioration du cadre existant par l'élaboration d'une réglementation complémentaire.

Concernant leur réglementation, les technologies de reconnaissance faciale sont aujourd'hui juridiquement bien encadrées au sein de l'Union européenne. Toutefois, ce que montre l'analyse juridique c'est un profond manque d'efficience dans l'application de ce cadre, en particulier en ce qui concerne le respect des droits fondamentaux. Il y a ici une voie cruciale d'amélioration, dont l'objectif doit être de contraindre tous les acteurs de l'écosystème des technologies de reconnaissance faciale à mieux appliquer le cadre existant, et ce dès l'expérimentation et les processus de mise sur le marché. Il convient également de considérer le caractère évolutif de ces technologies, pour garantir la robustesse d'un cadre protecteur dans la durée et éviter qu'il ne devienne vite obsolète.



En outre, il y a dans le déploiement des technologies de reconnaissance faciale de forts enjeux géopolitiques, allant de la compétition sur le marché mondial à la défense de la souveraineté européenne. Le débat offre une opportunité unique à l'Europe d'imposer ses propres règles afin non seulement d'accroître sa compétitivité face aux États-Unis et à la Chine, mais également de bâtir une voie européenne forte, porteuse de ses valeurs.

L'approche par la standardisation européenne se distingue dès lors comme la meilleure façon de s'engager dans cette voie. Élaborer nos propres standards nous donne une chance d'introduire le respect des droits fondamentaux au cœur du déploiement des technologies de reconnaissance faciale. Une telle initiative au niveau européen permettrait également d'assurer l'harmonisation et l'application efficiente du cadre juridique existant, tout en garantissant l'indépendance technologique de l'Union européenne. En matière de reconnaissance faciale, il est en effet grand temps que l'UE s'émancipe de la mainmise des États-Unis sur le marché international de la standardisation.

LA PRÉDOMINANCE DU NIST DANS LE MARCHÉ INTERNATIONAL DE LA STANDARDISATION

LES FONDEMENTS DE CETTE PRÉDOMINANCE : UNE COMPÉTENCE RECONNUE À L'INTERNATIONAL ET L'ABSENCE D'ÉQUIVALENT EUROPÉEN

En termes de biométrie, le National Institute for Standards and Technology (NIST) est devenu dans les années 2000 le centre de référence international de la standardisation. De concert avec l'industrie, cette agence du Département du Commerce américain procède régulièrement à des évaluations d'algorithmes et développe des normes et standards qui s'exportent ensuite à l'international. Du fait de ses liens avec l'industrie et des ponts qu'il a su construire avec le monde académique, le NIST est reconnu comme l'organe le plus compétent en la matière. Il est d'ailleurs fréquemment sollicité par le gouvernement américain pour réaliser des missions d'évaluation de performance d'algorithmes, y compris en matière de reconnaissance faciale. Ainsi, une grande légitimité est attribuée aux algorithmes bien placés dans les classements établis par le NIST, et la conformité aux normes et aux standards élaborés par l'agence américaine est devenue une priorité absolue pour de nombreux producteurs (pas seulement américains, mais également euro-

péens, russes et chinois[123]) de dispositifs de reconnaissance faciale. Les résultats du fameux *Facial Recognition Vendor Test* (FRVT) sont régulièrement cités par les fournisseurs de technologies comme une mesure de leur crédibilité et par les responsables politiques comme gage de leur qualité pour justifier d'y avoir recours[124].

Du fait de la diffusion en Europe de technologies reposant sur des algorithmes évalués par l'agence américaine, les critères pris en compte par cette dernière dans le cadre de ses tests se sont peu à peu installés comme la référence à l'échelle de l'UE. Si bien qu'à l'heure actuelle, les critères d'évaluation établis par le NIST sont souvent mis en avant dans les appels d'offres européens[125]. En outre, les entreprises européennes, y compris françaises, qui ont su s'imposer comme des leaders sur le marché international des technologies de reconnaissance faciale, sont celles ayant accepté les standards américains comme mètre étalon. Si ces firmes ont pu accéder au marché mondial et peu à peu gagner des parts de marché, c'est en respectant les normes du NIST.

Cette prédominance est également rendue possible par l'absence d'un équivalent européen au NIST. Le Comité européen de normalisation (CEN), qui rassemble les organismes nationaux de standardisation européens (par exemple l'AFNOR pour la France[126]), jouit en effet d'une moindre influence dans l'élaboration de standards supranationaux. Cette différence d'impact entre le NIST et le CEN est liée à plusieurs éléments. D'une part, le CEN n'est pas une agence gouvernementale. Il dépend des contributions de ses membres et, dans une moindre mesure, de la Commission européenne, pour son fonctionnement. Il dispose, dès lors, d'un budget relativement limité. D'autre part, dans le cadre de ses missions d'évaluation, l'agence américaine a accès aux immenses bases de données biométriques du gouvernement américain (fournies notamment par le FBI, le Département d'État et le Département de la Sécurité intérieure). Le NIST a ainsi constitué au fil du temps des bases de tests contenant des millions de données biométriques. En Europe, où il est difficile de rassembler ce genre de données, une telle montée en puissance et de tels effets d'échelle sont impossibles pour le CEN. Enfin, le NIST travaille également avec des commissions de normalisation internationales à l'élaboration de normes communes, ce qui accentue d'autant plus sa mainmise sur le marché international de la standardisation. Les moyens financiers du NIST et son haut niveau d'expertise lui permettent en effet de mobiliser des délégations conséquentes au sein de ces instances, et de remporter l'adhésion des plus petites délégations qui possèdent une moindre expertise et des budgets plus limités. L'agence américaine collabore notamment avec le Comité technique mixte 1 de l'ISO-IEC et plus précisément avec son sous-comité 37 dédié à la biométrie (voir l'encadré « Le SC-37 de l'ISO-IEC »).

123 « Technology: how the US, EU and China compete to set industry standards », *Financial Times*, 24 juillet 2019 : . https://www.ft.com/content/0c91b884-92bb-11e9-aea1-2b1d33ac3271

124 « How the US plans to crack down on Chinese facial recognition tech used to 'strengthen authoritarian governments' », *This Week in Asia*, 18 juin 2019 : https://www.scmp.com/week-asia/geopolitics/article/3014868/how-us-plans-crack-down-chinese-facial-recognition-tech-used

125 Au cours des auditions réalisées dans le cadre du présent rapport, un industriel a notamment souligné que l'on retrouve par exemple dans les appels d'offres européens des questions comme : *« Votre système est-il référencé dans le FRVT du NIST ? »*.

126 Pour la liste complète des membres du CEN, voir : https://standards.cen.eu/dyn/www/f?p=204:5:0::::FSP_ORG_ID,FSP_LANG_ID:,34&cs=1177845D46C9904580CCC631EC8FE906F

Le SC-37 de l'ISO/IEC[127]

Au-delà du CEN, certains organismes nationaux de standardisation européens se réunissent également dans le cadre du Comité technique mixte 1 de l'instance internationale de normalisation ISO-IEC consacré aux technologies de l'information, et plus particulièrement au sein du SC-37, le sous-comité dédié à la biométrie. Ce sous-comité comporte, en outre, six groupes de travail, dont un chargé de réfléchir aux « *aspects omnijuridictionnels et sociétaux de la biométrie* »[128]. Chaque pays représenté au sein du SC-37 y délègue une équipe à travers son unique adhérent à l'ISO (l'ANSI pour les États-Unis, l'AFNOR pour la France, le Deutsches Institut für Normung pour l'Allemagne, la British Standards Institution pour le Royaume-Uni, etc.)[129]. Ces équipes participent aux discussions techniques du sous-comité sur la base de contributions écrites. Les statuts du comité ISO/IEC prévoient une égale représentativité des pays (c'est-à-dire sans voix prépondérante dans la prise de décision et donc une représentativité quelle que soit la taille de la délégation). Toutefois, la taille des délégations n'est pas neutre dans le mécanisme

127 International Standardisation Organisation (ISO)/International Electronical Commission (IEC).

128 Pour de plus amples informations concernant le SC-37, voir : https://www.iso.org/fr/committee/313770.html

129 Pour la liste complète des membres du SC-37, voir : https://www.iso.org/committee/313770.html?view=participation

décisionnel. En effet, le détail des discussions techniques débouche souvent sur des arbitrages, si bien qu'au sein du SC-37 l'usage est de procéder aux décisions sur la base de la majorité des votes des délégations présentes en réunion. En l'absence d'un point de vue affirmé (du fait de l'étroitesse du champ de compétences), les petites délégations sont enclines à adopter une rationalité mimétique et à adosser leurs votes sur la confiance personnelle en certains délégués ou délégations, voire également en fonction du contexte politique du moment.

L'aspect financier n'est pas neutre, non plus, dans le fonctionnement de ces comités internationaux qui, pour élaborer une norme, s'appuient sur trois à quatre réunions annuelles, quelquefois étalées sur plusieurs années. Seules les grandes entreprises qui investissent dans la biométrie, les institutions d'une certaine envergure (le NIST, le Fraunhofer Institute) et les gouvernements significativement impliqués, mobilisent des délégués au sein de leur représentation au SC-37. La délégation américaine y est toujours très nombreuse. En plus des représentants de différents ministères fédéraux, on y retrouve la plupart des industriels américains producteurs de biométrie, qui y voient l'opportunité de promouvoir leur savoir-faire dans la construction des normes biométriques.

Depuis sa création en 2002, le SC-37 a mis au point pas moins de 130 normes internationales relatives à la biométrie. Si la majeure partie de ces normes n'est pas utilisée (à titre d'exemple, la norme sur les API[130] des capteurs biométriques n'a jamais vraiment eu le succès espéré), certaines d'entre elles sont effectives et largement appliquées mondialement. C'est le cas des normes ISO/IEC 19794-2, 19794-4, 19794-5 et 19794-6 relatives aux formats d'échange de données biométriques et qui sont reprises quasi systématiquement dans les appels d'offres comportant de la biométrie. La norme 19794-5 est par exemple celle qui définit les critères à respecter pour les photos utilisées sur nos titres d'identité[131].

Il y a donc là un enjeu crucial pour l'Union européenne, qui doit se donner les moyens de s'investir pleinement dans ces instances. Pour donner plus de force à cette action, la stratégie européenne doit être collégiale, plutôt que le fruit d'acteurs isolés issus des différents États membres.

130 *Application programming interfaces* ou interfaces de programmation en français.
131 Voir : https://www.diplomatie.gouv.fr/IMG/pdf/depliant_norme_photo-2.pdf

LA NÉCESSAIRE REMISE EN CAUSE DE CETTE PRÉDOMINANCE

Derrière cette prédominance se cachent deux enjeux pour l'Europe : maintenir une certaine indépendance technologique vis-à-vis des États-Unis, et adopter des valeurs qui ne sont pas nécessairement les nôtres. Dans l'écosystème numérique mondial, la prédominance des États-Unis et de la Chine, et le relatif retard technologique de l'Europe, posent la question de la maîtrise des données. Cet enjeu résonne avec une acuité toute particulière dans le cadre des technologies de reconnaissance faciale, ces dernières reposant sur le traitement de données biométriques, qui sont parmi les données les plus sensibles.

D'autre part, les critères établis et utilisés par le NIST, notamment dans le cadre du *Face Recognition Vendor Test (FRVT)*, très largement considéré comme le mètre étalon pour déterminer la fiabilité des logiciels de reconnaissance faciale[132], sont exclusivement techniques. Comme expliqué dans le rapport « Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects »[133] paru en décembre 2019, la performance des systèmes soumis au FRVT est principalement analysée selon un critère : la précision (« accuracy »)[134]. Cette précision, l'agence américaine en rend compte au travers d'un taux d'erreurs, c'est-à-dire le nombre d'erreurs de Type I ou « faux positifs » (un individu est incorrectement associé à un autre) et de Type II ou « faux négatifs » (un individu n'est pas associé à lui-même) commises par les algorithmes en question. Le temps d'exécution de l'algorithme et les « différentiels démographiques » (les variations de précision en fonction du groupe démographique[135]) sont également pris en compte. À l'issue du test, les algorithmes sont classés par le NIST, du plus performant au moins performant[136], sur la base de ces critères.

132 « How the US plans to crack down on Chinese facial recognition tech used to 'strengthen authoritarian governments' », *This Week in Asia*, 18 juin 2019 : https://www.scmp.com/week-asia/geopolitics/article/3014868/how-us-plans-crack-down-chinese-facial-recognition-tech-used
133 National Institute of Standardization and Technology (2019), « Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects » , U.S. Department of Commerce, 82 pp.
134 *Ibid.*, p. 20.
135 Les critères retenus pour évaluer ces « différentiels démographiques » sont l'âge, le sexe et le lieu de naissance (renvoyant à l'origine ethnique) des individus.
136 Pour un exemple de classement établi par le NIST, voir : https://pages.nist.gov/frvt/html/frvt11.html

Or, lorsqu'il s'agit de technologies de reconnaissance faciale, la fiabilité d'un système ne saurait s'arrêter à ses seules performances techniques. Si nous considérons la protection des données personnelles et le respect des droits fondamentaux comme des attributs essentiels, alors une technologie de reconnaissance faciale fiable n'est pas seulement une technologie performante. C'est une technologie en laquelle nous pouvons avoir confiance car elle ne mènera pas à l'usurpation de notre identité, au partage incontrôlé de nos données biométriques, à l'intrusion dans notre vie privée sans consentement préalable, ou à une surveillance massive et à distance de nos faits et gestes. Malgré les récentes initiatives du Sénat américain pour interdire les entreprises ne respectant pas les droits de l'homme de soumettre leurs algorithmes au FRVT[137], la route est encore longue. En tout état de cause, prendre en compte ces critères passe par l'établissement d'un cahier des charges intrinsèquement européen qui corresponde à notre vision de la société numérique : une société inclusive et respectueuse des droits et libertés fondamentales.

Comme ce fut le cas dans le domaine de la protection des données personnelles, cette situation offre une opportunité inédite à l'Europe de s'émanciper de la prédominance américaine, en proposant et promouvant ses propres standards, afin de protéger effectivement les droits de ses citoyens.

FAIRE DES STANDARDS EUROPÉENS LE LEVIER DE LA PROTECTION DES CITOYENS

Comme indiqué dans son préambule, l'objet de la Charte des droits fondamentaux de l'Union européenne est « *de renforcer la protection des droits fondamentaux à la lumière de l'évolution de la société, du progrès social et des développements scientifiques et technologiques* ». Si l'Union européenne veut s'assurer que ses valeurs et principes soient effectivement protégés et pris en compte dans le déploiement des technologies de reconnaissance faciale, elle doit s'investir plus massivement dans la course mondiale à la standardisation. Afin de s'imposer, l'Union européenne peut compter sur son *soft power* (voir l'encadré « Le *Brussels effect* »), comme elle a su le faire au travers de l'adoption du RGPD. Ce cadre pâtit toutefois des fluctuations dans son application d'un pays à l'autre. C'est pourquoi rapprocher les initiatives des différents États membres autour de cette standardisation doit être une priorité. Cela est d'autant plus important que, comme le souligne la Commission européenne dans son livre blanc sur l'intelligence artificielle, certains membres de l'UE se lancent déjà dans des initiatives unilatérales d'encadrement des applications de l'IA[138].

Le « *Brussels effect* »

Dans la course mondiale à la standardisation, l'Union européenne se distingue des deux autres grands pôles leaders sur le marché du numérique, que sont les États-Unis et la Chine. Alors que la Chine a adopté une stratégie agressive visant à pousser la diffusion de ses normes à l'échelle mondiale, et que l'administration Trump s'est engagée dans une véritable guerre économique avec cette dernière, l'Union européenne mise sur son *soft power* et plus particulièrement sur le *« Brussels effect »* pour imposer ses valeurs[139]. Ce terme mis en lumière par un journaliste du *Financial Times*, renvoie au fait que certaines règles établies par l'UE (notamment dans l'industrie automobile, chimique et alimentaire) aient petit à petit été adoptées dans le monde entier. Le RGPD en est l'exemple le plus récent dans le champ numérique : de nombreux pays à travers le monde mettent en œuvre des lois afférentes à la réglementation des données personnelles fortement inspirées du règlement européen. C'est également le cas de la Californie, qui prend souvent les devants en matière de réglementation aux États-Unis[140]. Reste à savoir si l'UE saura jouer de ce *« Brussels effect »* afin de s'imposer sur le marché mondial de la standardisation des technologies de reconnaissance faciale.

137 « Senators introduce bill to regulate facial recognition technology », *The Hill*, 14 mars 2019 : https://thehill.com/policy/technology/434166-bipartisan-senators-introduce-bill-to-regulate-facial-recognition

138 Commission européenne (2020), « Intelligence artificielle : Une approche européenne axée sur l'excellence et la confiance », p. 12 : « *La commission fédérale allemande pour l'éthique des données a préconisé un système de réglementation fondé sur cinq niveaux de risque, allant d'une absence de réglementation pour les systèmes d'IA les plus inoffensifs à une interdiction totale pour les plus dangereux. Le Danemark vient de lancer un prototype de label éthique en matière de données. Malte a mis en place un système volontaire de certification pour l'IA. Si l'UE ne se dote pas d'une approche européenne, il existe un risque réel de fragmentation du marché intérieur, ce qui porterait atteinte aux objectifs de confiance, de sécurité juridique et d'adoption par le marché* ».

139 « Technology: how the US, EU and China compete to set industry standards », *Financial Times*, 24 juillet 2019 : https://www.ft.com/content/0c91b884-92bb-11e9-aea1-2b1d33ac3271

140 *Ibid.*

PRENDRE EN COMPTE À LA FOIS LES ASPECTS TECHNIQUES ET JURIDIQUES

Alors que les standards américains qui prédominent actuellement le marché s'appuient exclusivement sur des caractéristiques ayant trait aux performances techniques des algorithmes, l'Europe doit se distinguer en introduisant dans ses propres standards une dimension juridique. Prendre en compte ces aspects est indispensable si nous entendons garantir un développement des technologies de reconnaissance faciale respectueux des valeurs européennes. En outre, les référentiels actuels, qui reposent sur de simples classements, sont perfectibles y compris du point de vue de la performance algorithmique. Dans le processus d'élaboration de standards européens applicables aux technologies de reconnaissance faciale, il est dès lors primordial de ne pas reléguer ces aspects au second plan.

Quel que soit l'usage qui est fait des technologies de reconnaissance faciale, il convient en effet de s'assurer de la loyauté des algorithmes, c'est-à-dire du fait qu'ils réalisent de la manière la plus performante possible les tâches pour lesquelles ils ont été conçus.

À cet égard, bien que le NIST, dans son FRVT, prenne en compte un certain nombre de critères (taux d'erreurs, temps d'exécution, différentiels démographiques) permettant de statuer sur la performance des algorithmes les uns par rapport aux autres et sur la performance d'un algorithme donné au fil du temps, l'agence américaine n'émet pas de certifications techniques. Les évaluations réalisées par le NIST n'ont en effet pas vocation à dire « tel système est conforme à nos standards, tel autre ne l'est pas ». Au lieu de cela, les algorithmes sont classés du plus performant au moins performant. Dès lors, comment déterminer les systèmes dont le niveau de performance est jugé « acceptable » pour un déploiement à grande échelle ? Faut-il considérer les 100 premiers du classement ? Les 500 premiers ? Les standards européens doivent ainsi reprendre comme base les critères techniques utilisés par le NIST, mais en y introduisant notamment des seuils évolutifs. Pour chaque critère analysé, que ce soit le taux d'erreurs, le temps d'exécution ou les différentiels démographiques, définir un seuil en dessous duquel le système est jugé non-conforme permettrait d'aboutir à des standards plus précis et de mettre en place un réel mécanisme de certification. Ainsi, les algorithmes classés en dessous du seuil (par exemple ceux dont les résultats en termes de gestion des biais discriminatoires sont jugés trop faibles) ne seraient pas certifiés. Afin de prendre en compte les évolutions technologiques réalisées au fil du temps, ses seuils doivent être évolutifs.

Si ces aspects techniques doivent constituer le premier pilier des standards européens applicables aux technologies de reconnaissance faciale, le deuxième pilier se compose lui d'aspects juridiques. Pour l'heure, ces derniers sont totalement absents des standards établis par le NIST.

En avril 2019, le groupe d'experts de haut niveau sur l'intelligence artificielle, mis en place par la Commission européenne, a publié ses « Lignes directrices en matière d'éthique pour une IA digne de confiance »[141]. Les experts identifient dans le document sept exigences essentielles pour l'IA, à savoir : (1) l'action humaine et le contrôle humain ; (2) la robustesse technique et la sécurité ; (3) le respect de la vie privée et la gouvernance des données ; (4) la transparence ; (5) la diversité, la non-discrimination et l'équité ; (6) le bien-être sociétal et environnemental ; et (7) la responsabilité[142]. Plus récemment, dans son livre blanc sur l'intelligence artificielle, la Commission européenne a repris un certain nombre de ces exigences en les précisant pour les applications d'IA dites « à haut risque ». On retrouve ainsi parmi les préconisations de la Commission la nécessité de mettre en place des exigences spécifiques pour l'identification biométrique à distance, notamment le respect de la Charte des droits fondamentaux[143].

141 Groupe d'experts indépendants de haut niveau sur l'intelligence artificielle constitué par la Commission européenne en juin 2018 (2020), « Lignes directrices en matière d'éthique pour une IA digne de confiance » : https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60427
142 *Ibid.*, p. 3.
143 Commission européenne (2020), « Intelligence artificielle : Une approche européenne axée sur l'excellence et la confiance », pp. 25-26.

Bien que ce qui constitue concrètement une application d'intelligence artificielle « à haut risque » reste à définir, la Commission européenne évoque dans son livre blanc l'exemple du déploiement des technologies de reconnaissance faciale dans les lieux publics[144]. Or, dans une approche par la standardisation, il n'y a pas lieu de distinguer entre les usages. Tous, quel que soit leur degré de sensibilité, doivent être encouragés à passer au crible de ces critères. En d'autres termes, toute mise en œuvre (y compris dans le cadre d'une expérimentation) d'un dispositif de reconnaissance faciale doit passer l'épreuve d'un test au regard des droits fondamentaux. À ce titre, chaque déploiement doit au préalable :

- être prévu par la loi ;
- répondre véritablement à des objectifs d'intérêt général reconnus par l'Union européenne ou à la nécessité de protéger les droits et libertés d'autrui ;
- respecter l'essence des droits et libertés, c'est-à-dire le noyau inaliénable du droit concerné ;
- être nécessaire (principe de nécessité) ;
- respecter le principe de proportionnalité (ce qui nécessite de passer l'épreuve du triple test)[145].

In fine, seules les technologies rassemblant toutes ces dimensions seraient jugées respectueuses de nos droits fondamentaux et pourraient être mises en œuvre.

144 *Ibid.*, p. 25.

145 Conformément au triple test, une mesure restrictive des droits fondamentaux doit être appropriée, nécessaire, et proportionnée.

TABLEAU 2 - LES CRITÈRES ESSENTIELS DES STANDARDS EUROPÉENS[146]

Critères techniques	Pour tous les usages : critères établis par le NIST (taux d'erreurs, rapidité d'exécution, différentiels démographiques) enrichis de seuils de performance évolutifs
Critères juridiques	Pour tous les usages : respect de la Charte des droits fondamentaux de l'UE Selon les usages : respect du RGPD ou de la Directive Police-Justice et autres normes propres aux États membres (par exemple, en France, la Loi Informatique et Libertés)

GARANTIR L'ADOPTION DES STANDARDS EUROPÉENS EN IMPOSANT LEUR RESPECT DANS LES MARCHÉS PUBLICS

En tout état de cause, la définition de standards visant à accompagner le déploiement des technologies de reconnaissance faciale sur le continent européen ne saurait être une fin en soi. Encore faut-il que ceux-ci remplissent effectivement leur mission : garantir l'harmonisation et l'efficacité dans l'application du cadre juridique existant. Dans la mise en œuvre concrète du système de standardisation, il convient donc de penser à la façon d'encourager le respect et la diffusion des standards. Ces derniers étant volontaires, cela doit s'inscrire dans une démarche performative.

146 Notons que nous n'évoquons pas parmi les critères essentiels certains grands principes inhérents à toute technologie reposant sur l'intelligence artificielle ou le numérique en général. Il va cependant de soi que, autant que faire se peut, les technologies de reconnaissance faciale utilisées sur le continent doivent également intégrer dans leur fonctionnement le principe de « technologie verte », en accord avec le Pacte Vert pour l'Europe *(European Green Deal)* présenté par la Commission européenne en décembre 2019.

Il s'agirait en premier lieu d'imposer le respect des standards dans le cadre des marchés publics européens, nationaux et locaux, expérimentations incluses. Concrètement, il s'agit d'octroyer des marchés publics aux seules organisations respectant les standards en question, pour toutes les technologies de reconnaissance faciale, quel que soit le degré de risque. Cette obligation permettrait de se prémunir des initiatives qui éclosent aujourd'hui dans les territoires sans contrôle effectif et sans recherche d'alternatives. Pour ce faire, les appels d'offres devraient contenir des critères permettant d'évaluer les solutions proposées par rapport aux standards européens. Le fait de ne pas respecter les standards serait préjudiciable pour les opérateurs présents sur le marché (et ceux souhaitant y entrer), et ces derniers se verraient incités à les respecter soit en les prenant en compte lors de la phase de développement de leurs dispositifs, soit en passant par une mise en conformité des dispositifs existants.

Ce « nivellement par le haut » devrait avoir un effet performatif et permettre aux standards européens de devenir le référentiel à respecter pour le déploiement de technologies de reconnaissance faciale au sein de l'UE, que leurs fabricants y soient basés ou non, et que les marchés soient publics ou privés. Par ailleurs, outre leur diffusion, notons que l'imposition des standards dans le cadre des marchés publics permettrait dès lors un encadrement effectif de la surveillance publique. L'étape ultime de l'adoption des standards européens en matière de reconnaissance faciale serait leur diffusion internationale au travers du fameux *« Brussels effect »*.

Tout ceci nécessite toutefois de pouvoir contrôler le respect des standards au niveau de l'UE, ce qui sous-entend que des organismes européens soient à même d'une part de les porter et d'autre part de les auditer.

UNE GOUVERNANCE EUROPÉENNE DÉDIÉE À LA STANDARDISATION DES TECHNOLOGIES DE RECONNAISSANCE FACIALE

Alors que le cadre actuel des technologies de reconnaissance faciale se caractérise par une application disparate à l'échelle de l'Union, l'élaboration d'un référentiel commun à l'ensemble des États membres passe inévitablement par une mise en commun des connaissances de tous les acteurs pertinents au sein d'une instance multi-parties prenantes chargée de porter ces standards.

RÉUNIR LES EXPERTISES AU SEIN D'UNE INSTANCE MULTI-PARTIES PRENANTES

Bien qu'il convienne de le revisiter, l'écosystème des acteurs susceptibles d'être impliqués dans le contrôle des standards européens afférents au déploiement des technologies de reconnaissance faciale n'est pas complètement à construire. Pour l'heure, ce dernier se matérialise essentiellement par un réseau d'autorités nationales chargées de la protection des données et d'organismes nationaux de standardisation que nous retrouvons au niveau européen au sein de diverses instances. L'instance chargée de porter les standards européens en matière de reconnaissance faciale doit s'appuyer sur ces organes pour l'élaboration d'un référentiel commun à l'ensemble des États membres[147].

Elle pourrait notamment s'appuyer sur le Comité européen de normalisation (CEN), qui rassemble les organismes nationaux de standardisation des États membres et dont la mission première est la production de standards de sécurité et de qualité européens. Cet organisme porte en outre des réflexions relatives aux technologies de reconnaissance faciale depuis plusieurs an-

147 Ce principe selon lequel il convient de s'appuyer en priorité sur les organes existants a par ailleurs été rappelé le 12 mai dernier au sein de la commission « JURI » de la Commission européenne par les rapporteurs fictifs des groupes PPE, Renew, ECR, et ID. Ces derniers se sont en effet opposés à l'idée de créer une « agence européenne pour l'IA » défendue par l'eurodéputé Iban Garcia del Blanco (S&D) et proposent plutôt de s'appuyer sur les autorités existantes. Voir : https://multimedia.europarl.europa.eu/fr/juri-committee-meeting_20200512-0900-COMMITTEE-JURI_vd

nées, mais qui méritent une réactualisation. Dans son rapport d'activité pour l'année 2016, le Comité annonçait avoir validé un programme de travail visant à atteindre « *un accord sur l'élaboration prochaine d'une norme européenne sur la « protection de la vie privée dès la conception et par défaut »* (privacy protection by design and by default*) et sur des lignes directrices spécifiques au secteur pour la surveillance vidéo (CCTV) et des mesures biométriques pour le contrôle d'accès, y compris la reconnaissance faciale.* »[148] Si le volet sur la protection de la vie privée dès la conception et par défaut a depuis été repris par le Comité européen de la protection des données (EDPB)[149], celui sur la biométrie semble avoir été quelque peu délaissé[150].

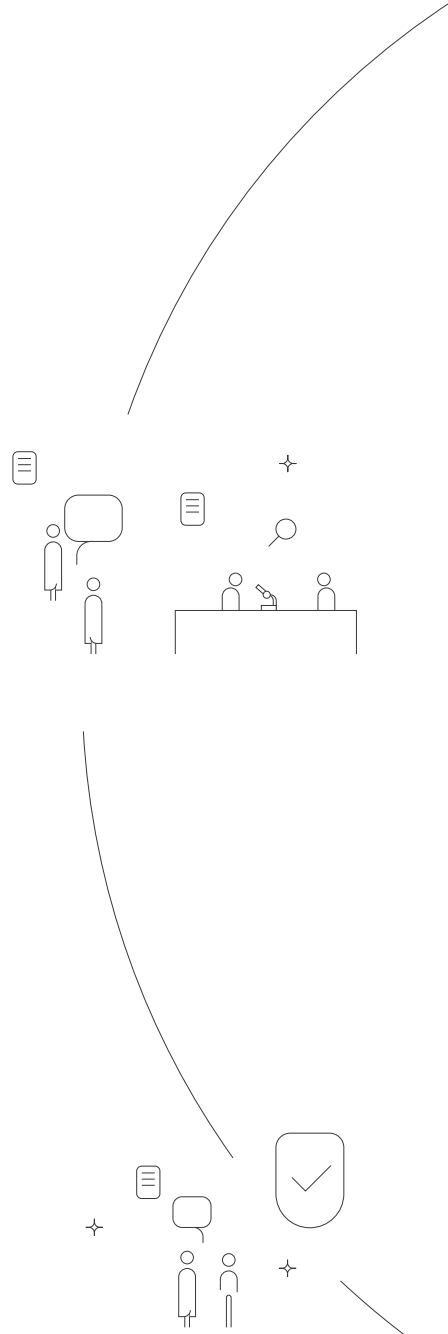
En plus des organismes nationaux de standardisation, il est crucial d'impliquer dans cette instance des représentants de l'EDPB[151], c'est-à-dire des autorités nationales chargées de la protection des données (la CNIL pour la France et ses équivalents européens)[152]. La protection des données biométriques, données hautement sensibles, doit en effet être au cœur du système de standardisation européen.

L'élaboration de standards européens ayant également vocation à prendre en compte le respect des droits fondamentaux, il est essentiel que les représentants du CEN et de l'EDPB collaborent étroitement avec les experts de l'Agence des droits fondamentaux de l'UE au sein de cette instance. Cette dernière fournit des conseils d'experts indépendants et des analyses en matière de droits fondamentaux aux institutions de l'UE et aux États membres. Elle est l'organe le plus à même de contribuer à la vulgarisation du triple test. L'Agence des droits fondamentaux de l'UE entretient en outre des relations de travail particulièrement étroites avec les autorités nationales en charge de la défense des droits, qu'il est indispensable d'impliquer dans l'élaboration des standards européens afférents aux technologies de reconnaissance faciale. En France, le Défenseur des droits protège notamment les droits des usagers des services publics et les droits de l'enfant, et lutte activement contre les discriminations.

148 Comité Européen de Normalisation (2017), Rapport annuel 2016, p. 9 : https://www.cen.eu/news/brochures/brochures/Rapport%20annuel%202016%20Tome%201%20FR%20accessible.pdf
149 European Data Protection Board (2019), « 2018 Annual Report : Cooperation & Transparency », p. 25 : https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_annual_report_2018_-_digital_final_1507_en.pdf
150 Il n'en est fait aucune mention dans les rapports d'activités du CEN pour 2017 et 2018.
151 À ne pas confondre avec le Contrôleur européen de la protection des données (CEPD).
152 Pour la liste complète des membres de l'EDPB, voir : https://edpb.europa.eu/about-edpb/board/members_fr

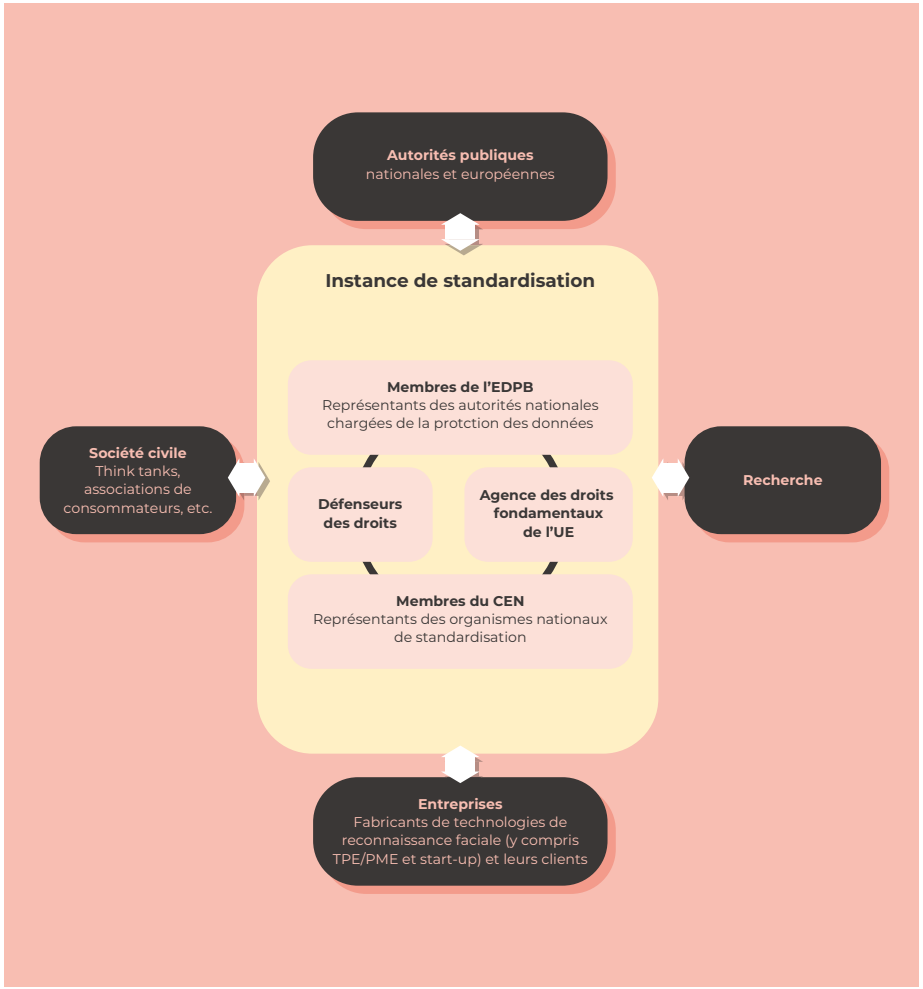
Cette mise en commun des connaissances et des compétences en vue d'élaborer des standards européens et de les rendre compréhensibles pour les industriels comme pour les autorités de contrôle, pourrait nécessiter la création de groupes de travail, chacun dédié à une thématique spécifique (par exemple les aspects techniques, la protection des données, les droits fondamentaux, des droits transverses, la transparence, etc.).

Pour que le système soit réellement complet et démocratique, il convient en outre que les réflexions menées par l'instance de standardisation s'inscrivent dans une logique de consultation de la société civile (think tanks[153], associations de consommateurs, associations de défense des droits), du monde de la recherche, des entreprises et d'autres autorités publiques sur la mise en œuvre des standards et leur développement ultérieur (voir le Graphique 3 « La structure de l'instance européenne de standardisation des technologies de reconnaissance faciale »). Afin d'éviter les doublons, il conviendrait également que ce travail soit mené main dans la main avec les directions générales pertinentes de la Commission européenne[154].



153 Par exemple le *Biometric Institute*, qui travaille beaucoup sur le sujet.
154 La DG Justice travaille par exemple actuellement à l'élaboration d'un étalon sur la reconnaissance des empreintes digitales.

GRAPHIQUE 3 - LA STRUCTURE DE L'INSTANCE EUROPÉENNE DE STANDARDISATION DES TECHNOLOGIES DE RECONNAISSANCE FACIALE



Toutefois, si contrôler le respect des standards au niveau de l'UE nécessite une instance dédiée à leur élaboration, cela demande aussi que ces standards puissent être audités.

PLACER L'AUDITABILITÉ AU CŒUR DU SYSTÈME DE STANDARDISATION

L'auditabilité est la raison d'être de tout système de standardisation. Si nos standards ne sont pas auditables, nous n'avons aucun moyen de contrôler leur respect. Établir ces derniers doit donc permettre d'élaborer un référentiel de certification[155] commun à l'ensemble de l'UE. Ainsi, le référentiel de certification des technologies de reconnaissance faciale européen doit comprendre la liste des exigences à contrôler, traduisant de façon claire et abordable les normes instaurées consensuellement par l'instance de standardisation.

Une fois le référentiel établi, c'est-à-dire une fois les principes juridiques (notamment le triple test) et les aspects techniques traduits sous forme d'exigences pratiques, il devient possible pour un organisme de contrôle européen d'auditer un dispositif en vue de le certifier. C'est là que l'idée d'imposer les standards dans les marchés publics prend tout son sens. Si un fabricant de technologie de reconnaissance faciale espère que son dispositif soit retenu lors d'un appel d'offres public, alors il aura tout intérêt à le faire certifier par un organisme indépendant compétent. Sans cette certification, sa proposition ne sera pas retenue.[156] Ce mécanisme permet à la fois à l'entreprise ou à l'autorité ayant recours à une technologie de reconnaissance faciale de prouver qu'elle respecte les normes établies, et de garantir aux citoyens que le dispositif auquel ils sont soumis est digne de confiance (non seulement d'un point de vue technique, mais également éthique).

Notons ici qu'une certification est accordée pour une durée limitée, pendant laquelle l'organisme certificateur exerce une surveillance. Par ailleurs, les technologies de reconnaissance faciale étant des dispositifs qui évoluent constamment au gré des innovations, peut-être faudrait-il envisager un

155 C'est-à-dire un *« document technique définissant les caractéristiques que doit présenter un produit industriel ou un service et les modalités du contrôle de la conformité à ces caractéristiques »*. Voir Ministère de l'Économie, des Finances et de l'Industrie (2004) : « La certification en 7 questions des produits industriels et des services », p.4. : https://evaluation.cstb.fr/doc/certification/certification-en-7-questions.pdf

156 Notons qu'il convient de veiller à ce que le système de standardisation ne devienne pas une barrière pour les nouveaux entrants. Toutes les entreprises, des TPE jusqu'aux multinationales, doivent être en mesure de développer des technologies conformes aux standards. D'où la nécessité de consulter également les plus petits acteurs dans la mise en œuvre et le développement ultérieur des standards (voir Schéma « La structure de l'instance européenne de standardisation des technologies de reconnaissance faciale »).

mécanisme de notification destiné à prévenir l'organisme certificateur des évolutions dans le temps d'une technologie qu'il a certifiée. Il s'agirait pour le fabricant de la technologie de prévenir l'organisme de toute modification conséquente apportée au dispositif en question, en vue d'une réévaluation de la certification. Ce suivi devrait se concentrer sur les évolutions significatives portant sur la fonctionnalité du produit, susceptibles de modifier sensiblement ses performances lors des tests ou la nature des informations de sécurité à fournir. Les mises-à-jour telles que les correctifs de sécurité ou les améliorations simples ne doivent pas déclencher une nouvelle évaluation des risques après la mise sur le marché d'une technologie.

Ce contrôle de conformité nécessite toutefois de pouvoir comparer les algorithmes sur lesquels reposent les technologies de reconnaissance faciale à des bases de données d'images conséquentes et centralisées, chose particulièrement difficile au sein de l'UE à l'heure actuelle. Bien que la réglementation européenne le permette à certaines conditions, plusieurs principes du RGPD créent une antinomie à la création de grandes bases de données centralisées. À cet effet, il est nécessaire que l'Union européenne développe une doctrine visant à encourager les innovations en matière d'intelligence artificielle, tout en préservant les principes essentiels du RGPD.

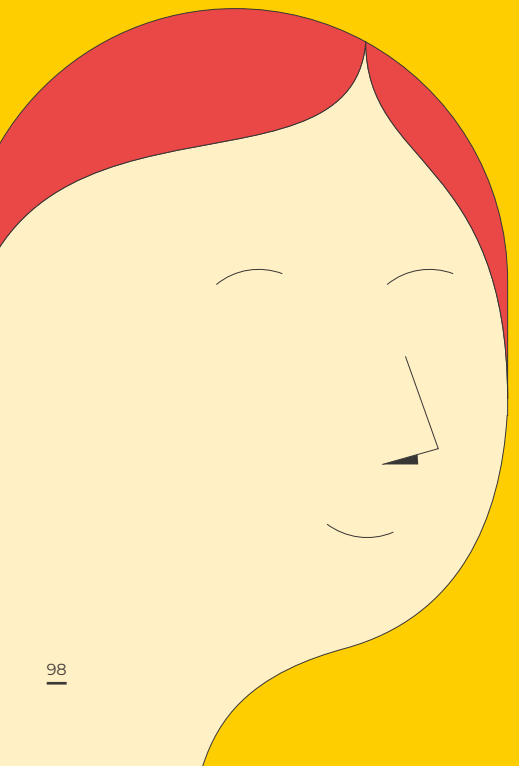
Au-delà de la mise en place de ce mécanisme de certification qui repose sur l'audit par des tiers (bureaux/organismes indépendants certificateurs), le fait d'avoir un référentiel au niveau européen permettrait également l'auto-auditabilité des sociétés qui développent et/ou ont recours aux technologies de reconnaissance faciale. Ces dernières doivent en effet pouvoir s'approprier le référentiel en vue de procéder à des analyses d'impact *a priori*. La possibilité de cette auto-évaluation par rapport au référentiel est d'autant plus nécessaire depuis la disparition quasi généralisée du régime de l'autorisation préalable avec l'entrée en vigueur du RGPD. Alors que ce n'est actuellement pas le cas, nous pourrions imaginer de rendre obligatoire la transmission de ces analyses d'impact aux autorités de contrôle nationales (à la CNIL, par exemple), afin que celles-ci émettent des avis. L'auto-auditabilité n'a cependant pas vocation à se substituer à la certification par des tiers. Elle est une démarche volontaire de la part du fabricant lui permettant de prendre en compte dès la conception les exigences du référentiel européen. Le processus de certification ayant un coût, il est primordial pour un industriel de s'assurer que sa demande de certification ait le plus de chances possibles d'être acceptée.

Enfin, en plus des tiers certificateurs et des fournisseurs de technologies, les autorités chargées de contrôler le respect des normes doivent également pouvoir s'approprier le référentiel. Ceci est indispensable non seulement en vue de la généralisation du recours au triple test (aspect juridique), mais également en vue d'accroître l'efficacité du contrôle des aspects techniques. Dès lors, une montée en puissance des régulateurs est nécessaire. Réaliser des analyses d'impact portant sur des technologies complexes est une tâche extrêmement chronophage et qui requiert énormément de ressources, non seulement budgétaires mais également (et de façon tout aussi importante) humaines (personnel hautement qualifié). Force est de constater que, dans l'état actuel des choses, ces ressources sont loin d'être acquises[157]. Il est urgent que les États membres fassent montre d'une réelle volonté politique et dotent leurs autorités de contrôle des moyens dont elles ont besoin. Outre des moyens financiers, cela nécessite également un effort significatif de formation.

> Si la mise en place de ce système européen de standardisation se distingue comme l'option la plus à même de garantir un déploiement des technologies de reconnaissance faciale respectueux des valeurs européennes, concrétiser ce projet ne sera pas aisé. Une coopération accrue entre autorités nationales au sein d'une instance européenne, ainsi que des investissements (financiers et en ressources humaines) de la part des États membres apparaissent comme les conditions *sine qua non* du succès d'une telle entreprise. Échouer dans cette mission participerait de l'érosion de la souveraineté numérique européenne et de la potentielle mise à mal des garanties démocratiques de l'État de droit. Difficile donc d'envisager cette option.

157 *Brave, op. cit.*

CONCLUSION
L'OPPORTUNITÉ POUR L'UE DE REMETTRE L'HUMAIN AU CŒUR DU SYSTÈME



Au vu de l'actuelle prédominance de la standardisation américaine et alors que le déploiement de dispositifs de reconnaissance faciale s'accélère à l'échelle internationale, il est crucial que l'Union européenne se dote d'un système garant de ses valeurs. Il est en effet estimé que d'ici à 2024, le marché des technologies de reconnaissance faciale génèrera des revenus à hauteur de 7 milliards de dollars, soit plus de deux fois la valeur enregistrée pour 2019 (3,2 milliards)[158].

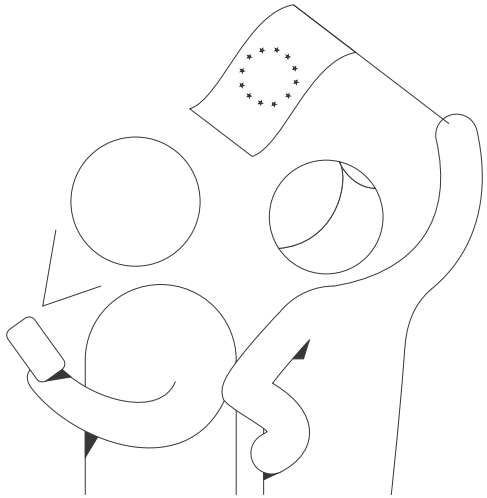
Au-delà de la garantie des droits des citoyens, il y a donc également, dans la mise en place de standards européens applicables aux technologies de reconnaissance faciale, un enjeu important de souveraineté numérique.

Toutefois, la stratégie européenne ne peut reposer sur la seule mise en place de standards européens auditables. En plus d'établir un système de standardisation garantissant une technologie de confiance, l'enjeu essentiel est de donner la maîtrise à l'humain. Qu'ils soient des acteurs publics ou privés, les utilisateurs des technologies de reconnaissance faciale participent grandement au déploiement de ces dernières dans les territoires. À ce titre, le caractère hautement sensible et intrusif de ces technologies doit toujours les inviter à se poser la question de l'alternative. Il convient également de s'assurer, y compris dans le domaine privé, que les individus soient mis en capacité d'interagir de la meilleure manière possible avec ces technologies. À cet égard, il est de la responsabilité des utilisateurs d'informer ex-

158 « Facial Recognition Market by Component (Software Tools (2D Recognition, 3D Recognition, and Facial Analytics) and Services), Application Area (Emotion Recognition, Access Control, and Law Enforcement), Vertical, and Region - Global Forecast to 2024 », *Markets & Markets*, juin 2019 : https://www.marketsandmarkets.com/PressReleases/facial-recognition.asp

plicitement les citoyens du déploiement d'un dispositif de reconnaissance faciale, afin que ces derniers puissent décider en toute conscience de soumettre ou non leur visage à un traitement biométrique. Une campagne de sensibilisation au niveau européen devrait également être déployée, dans le but d'informer les citoyens et leur permettre de mettre en œuvre leurs droits. Il est primordial que chaque individu soumis (de façon volontaire ou non) à un dispositif de reconnaissance faciale comprenne quels sont ses droits et ses voies de recours, où vont ses données, à quelles fins, par qui elles sont traitées, pour combien de temps, quels risques il encourt, etc.

Le 20 février dernier, la Commission européenne ouvrait à consultation publique son livre blanc sur l'intelligence artificielle dans lequel était annoncée (entre autres) sa volonté de lancer un vaste débat sur les technologies de reconnaissance faciale. Renaissance Numérique espère que les propositions concrètes formulées ici contribueront à un débat public éclairé et à garantir un déploiement des technologies de reconnaissance faciale en accord avec les valeurs qui forment la pierre angulaire de l'Union européenne.



REMERCIEMENTS

Nous remercions pour leur contribution, les différents acteurs qui ont participé aux auditions, à savoir :

Didier Baichère, Député des Yvelines

Vincent Bouatou, Directeur Innovation, Idemia

Antoine Courmont, Chargé d'études, CNIL

Théodore Christakis, Professeur de droit international, Université Grenoble Alpes

Martin Drago, Juriste, La Quadrature du Net

Raphaël de Cormis, Vice-président Innovation et Transformation numérique, Thalès

Marie Duboys Fresney, Conseillère juridique, CNIL

Arthur Messaud, Analyste juridique et politique, La Quadrature du Net

Henri Verdier, Ambassadeur pour le Numérique

Nous remercions également les équipes du Défenseur des Droits et de la Ligue des droits de l'Homme pour nos discussions nourries autour de ces enjeux.

Nous tenons enfin à remercier chaleureusement les intervenants et participants au colloque du 19 décembre 2019 à l'Assemblée nationale, et tout particulièrement Monsieur Jean-Michel Mis, Député de la Loire, avec qui nous avons co-organisé cette rencontre.

EN SAVOIR PLUS

« Reconnaissance faciale : Ce que nous en disent les Français », Renaissance Numérique (décembre 2019)

« Reconnaissance faciale : Interdiction, expérimentation, généralisation, réglementation. Où en est-on ? Où allons-nous ? », actes du colloque du 19 décembre 2019 à l'Assemblée nationale, Renaissance Numérique (février 2020)

DIRECTION DE LA PUBLICATION

Henri Isaac, Président, Renaissance Numérique

Camille Vaziaga, Responsable des affaires publiques, Microsoft France

COORDINATION

Jennyfer Chrétien, Déléguée générale, Renaissance Numérique

Jessica Galissaire, Responsable des études, Renaissance Numérique

RÉDACTEURS

Valérie Fernandez, Professeure et Titulaire de la chaire Identité Numérique Responsable, Telecom Paris

Jessica Galissaire, Responsable des études, Renaissance Numérique

Léo Laugier, Doctorant en informatique, Institut Polytechnique de Paris

Guillaume Morat, Senior Associate, Pinsent Masons

Marine Pouyat, Consultante indépendante experte en protection des données, marine-talents.com

Annabelle Richard, Avocate associée au pôle Technologies, Médias et Télécommunications, Pinsent Masons

LE GROUPE DE TRAVAIL

Sarah Boiteux, Senior Analyst en affaires publiques, Google France

Hector de Rivoire, Responsable des affaires publiques, Microsoft France

Etienne Drouard, Avocat associé, Hogan Lovells

Valérie Fernandez, Professeure et Titulaire de la chaire Identité Numérique Responsable, Telecom Paris

Léo Laugier, Doctorant en informatique, Institut Polytechnique de Paris

Guillaume Morat, Senior Associate, Pinsent Masons

Delphine Pouponneau, Directrice Diversité et Inclusion, Orange

Marine Pouyat, Consultante indépendante experte en protection des données, marine-talents.com

Philippe Régnard, Directeur des affaires publiques de la Branche numérique, La Poste

Annabelle Richard, Avocate associée au pôle Technologies, Médias et Télécommunications, Pinsent Masons

Thierry Taboy, Vice-président Responsabilité sociale d'entreprise, Orange

Amal Taleb, Directrice des affaires publiques, SAP France

Valérie Tiacoh, Directrice Communication Responsabilité sociale d'entreprise, Orange

RENAISSANCE
numerique

À PROPOS DE RENAISSANCE NUMÉRIQUE

Renaissance Numérique est le principal think tank français indépendant dédié aux enjeux de transformation numérique de la société. Réunissant des universitaires, des associations, des grandes entreprises, des start-ups et des écoles, il vise à élaborer des propositions opérationnelles pour accompagner les acteurs publics, les citoyens et les acteurs économiques dans la construction d'une société numérique inclusive.

Renaissance Numérique
22 bis rue des Taillandiers - 75011 Paris
www.renaissancenumerique.org

Juin 2020
CC BY-SA 3.0